Supplement A
to the Navy Enterprise Application Developer Guide (NEADG)

NMCI RD²G v1.1

NMCI Release Development and Deployment Guide

March 17, 2003

Change History

The following Change History log contains a record of changes made to this document. Entries should be made in descending order, with most recent changes at the top of table.

Published / Revised Date	Version # [*0.XX for unpublished documents*]	Author(s)	Section / Nature of Change
17 Mar 2003	v1.1	NRD²G Working Group	Review and revision
20 Dec 2002	DRAFT v1.1	NRD²G Working Group	Major Revision and Update
30 Sept 2002	DRAFT v1.0	Steven Baracosa in collaboration with others	Initial of version of revised guide taken from ARG and NEADG

DOCUMENT PROPERTIES
Owner: Director NMCI
Please send feedback on this version of the NRD²G in the suggested format below to:
NMCI PMO Developer Guidance Support
baracosas@saic.com
858-826-5872
Format:

Paragraph #	Problem/Concern	Recommended Solution

Your comments and recommendations to improve this guide are highly encouraged. As you review its contents consider these questions:

Does this guide give you what you need?

Does this guide overly constrain you and how?

In your response please ensure that you clearly reference the paragraph being addressed, explain the problem or concern and provide a recommended solution.

TABLE OF CONTENTS

Section **Page**

APPENDICES

Page

LIST OF FIGURES

Page

1.0 INTRODUCTION

The Navy Marine Corps Intranet (NMCI) is an Information Technology (IT) initiative and procurement strategy to provide secure, seamless, global end-to-end connectivity for Naval and Marine Corps warfighting and business functions. When completed, NMCI will consolidate Navy and Marine Corps computer networks into a single, secure, enterprise-wide managed service for voice, video and data information exchange. *Figure 1-1* provides an overview of the NMCI Infrastructure Architecture.

For the context of this guide, a release includes the introduction of a new application or a change to an existing application. A change can be identified as a software patch, fix, update, upgrade, modification, revision, or new version to an existing application that operates within NMCI.

1.1 PUPROSE

The purpose of this guide is to provide detailed information and guidance to application developers interested in migrating content, introducing new applications or changing existing applications within NMCI. This guide is written to support required activities within the overall NMCI Release Management Process (NRMP) that is in the development stage.

The NMCI Release Development and Deployment Guide (NRD^{2}G) is a consolidated source of information, guidance and direction to developers and application owners who build and/or modify applications as well as the acquirers of applications intended for use within NMCI. With the Navy Enterprise Portal (NEP) initiative under Task Force Web (TFW) on the horizon, this guide is intended to provide guidance for NMCI application maintenance and implementation during the interim period until the TFW initiative is complete. As a supplement to the Navy Enterprise Application Development Guide (NEADG), the NRD^{2}G is written to support the Central Design Authority (CDA) in the development and deployment of releases that will operate within NMCI. For web based application guidance, the user should refer to the NEADG, the TFW and NEP.

This document is a collaborative effort between the Information Strike Force (ISF) and the Department of the Navy (DON). The NRD^{2}G is intended to be a work in progress with enhancements inserted as required to support the current state of NMCI implementation.

The NRD^{2}G includes an overview of the NMCI infrastructure architecture and discusses the requirements necessary to develop, certify and deploy new/emerging applications, or to modify an existing application so that it is compatible with, and can be included in, the NMCI enterprise. Further, it contains a checklist that developers of applications must follow as the application goes through its development or modification process in order to ensure the application will meet all NMCI acceptance criteria. Additional NRD^{2}G sections address standards/programming practices, processes, and miscellaneous topics such as reusable components, metrics, and timelines. The guide concludes with resource appendices.

1.1.1 Legacy Applications Transition Guide (LATG)

For the purposes of this guide, Legacy Applications refer to any customer software application that exists prior to Site Cutover that is not included in the NMCI standard seat services or the Contract Line Item Number (CLIN) 0023 catalog. The NMCI Legacy Application Transition Guide (LATG) provides the detailed guidance to be used to transition DON legacy applications into the NMCI environment. Legacy Applications transition is beyond the scope of this guide. The LATG is found at http://www.nmci-isf.com/legacy_applications_transition_guide.pdf.

1.1.2 Navy Release Management Process (NRMP)

Developers must be aware that their release of new or update applications is part of the overall Navy Enterprise application management system and will be scrutinized as such. The NRMP (currently being developed) is designed to provide a structured approach to software application management across the enterprise. The NRMP will provide the necessary management and discipline needed to maintain and control enterprise size, configuration and security of Navy and Marine Corps applications. The purpose of the NRMP is to eliminate the proliferation of unnecessary, redundant and excess applications that are inherent in legacy systems. As part of the NRMP, all releases are subject to an executive review and approval for appropriateness within the enterprise. The NRMP has many steps that must be completed prior to approving the development and subsequent deployment of a release within NMCI. An entering assumption for using the NRMP is that the application release is appropriate and has received Navy executive level approval in accordance with the NRMP. Therefore, this guide will not address the NRMP and its approval steps.

1.2 OBJECTIVES

This guide describes the technical and management direction an application developer must follow to successfully develop, modify and deploy releases intended to operate within NMCI. By providing sufficient information, this document seeks to reduce the time and cost of developing or modifying, and deploying application releases. As a consolidated resource, the NRD²G eliminates the confusion of multiple documents that address only portions of the release development process for applications that will operate within NMCI.

1.3 SCOPE

This guide includes information on the processes required for Preparation, Pre-certification, Collection and Submission, ISF Packaging and Certification, Accreditation and Risk Mitigation, and Deployment of application releases intended for operation within NMCI. Additionally, this document presents methods, processes, procedures and interfaces for use by applications that extend beyond NMCI boundaries as well as applications owned and operated by other agencies, services, contractors or joint commands that need to be accessible by NMCI users.

The scope of this guide is limited and makes assumptions about the target audience and the level of knowledge within the developer community. References to web sites that provide detailed information about the technologies, standards, interfaces, and protocols used are provided in the list of references.

1.4 ROLES AND RESPONSIBILITIES

1.4.1 Director NMCI

Director, NMCI, is managing the acquisition of NMCI. The Director NMCI works for the Assistant Secretary of the Navy for Research Development and Acquisition (ASN RDA). Director NMCI works within the policy constraints of Department of Defense (DoD) acquisition regulations and provides additional acquisition guidance to the Navy and Marine Corps NMCI Program Managers.

1.4.2 Navy Information Officer (IO)

The Navy Information Officer (IO) is responsible for bring operational information technology/ information management (IT/IM) requirements into alignment with Navy functionality capabilities using developing and established processes and procedures. He advises and assists the Chief of Naval Operations (CNO) in achieving network-centric operational capabilities by managing robust global and local networks, employing proven-successful business practices and integrating IT/IM as it applies to warfighters at sea and the supporting shore establishment. He oversees the integration of dispersed sea-based and Joint command and control architectures as well as championing the incorporation of significant industry improvements in IT, in the areas such as supply chain and enterprise resource management, into the Navy enterprise.

The Navy IO leads the development of strategic plans and implementation strategies for managing global Navy enterprise IT solutions across the Navy. The Navy IO receives requirements from and provides policies and procedures to Commander, Naval Network Warfare Command (NETWARCOM) who is responsible for their implementation.

The Navy IO is tasked with the reduction of legacy applications and databases in order to support the rapid transition to NMCI. Navy IO works with and provides guidance to the functional area managers (FAMs) who are ultimately responsible for determining the suite of approved applications and databases used in their business area in order to accomplish the mission. Navy IO works with (Program Executive Office for Information Technology) PEO-IT to determine the policies and processes for procuring enterprise licenses for applications that have a significant user base across the naval enterprise, leveraging the capabilities of the Navy Marine Corps Intranet to enhance operations and communications within the Navy. In addition, the Navy IO is responsible for the following:

- Ensure IT/IM requirements are consistent and compliant with overall Navy/ DoD Joint architectures and investment decisions. The Navy IO will work closely with the DON and the U.S. Marine Corps (Chief Information Officer) CIOs to manage “Information” and “Knowledge” as key strategic resources in order to satisfy Fleet information requirements.
- Oversee the development and implementation of systems, policies and processes that will assure the integrity, availability, authentication and safeguarding of Navy information and information display, processing, and storage systems. Ensure Navy compliance with evolving national security information assurance (IA) policies through the acquisition and implementation of approved IT/IM products.

- Establish, manage, and enforce IT/IM configuration standards for hardware, software, and network connectivity. Oversee the development of an enterprise management process for IT/IM configuration control.
- Provide Navy leadership in support of DoD and DON CIOs' efforts to develop, maintain, implement, and evolve DoD Joint information architectures. Serve as the Navy's lead point of contact (POC) for interaction and coordination with other Service, Joint, DoD, and interagency CIOs for implementing the Global Information Grid enterprise solutions.
- Develop, coordinate, and ensure compliance with the Navy's IT/IM Plan that serves as a key input to the DON IT/IM Strategic Plan. The term "information technology" includes "national security systems" as defined in the Clinger-Cohen Act of 1996.
- Advise the CNO and other senior leadership on all IT/IM-related issues. Key to this function is close coordination and frequent liaison with DON and U.S. Marine Corps CIOs, the Fleet Commanders, Systems Commanders, Commander NETWARCOM, and other Major Claimant CIOs.
- Support DoD and DON CIO's efforts to promote effective and efficient design and operation of information management processes throughout the global Navy enterprise.
  Review and critique all Navy IT/IM Support Plans (C4I Support Plans), prepared and updated at each acquisition milestone in accordance with DoD 5000-series directives, to verify compliance with DoD Joint Technical Architectures and to ensure interoperability, compatibility and integration with other Joint warfighting and support systems.
- Oversee the implementation of a Navy-wide IT/IM systems-of-systems testing program to ensure continued interoperability.
- Develop and implement knowledge management strategies that facilitate the improved creation and sharing of knowledge. Knowledge management, which involves delivering the right information to the right decision-maker at the right time to create the right conditions for new knowledge, enables more effective and agile decision-making, resulting in greatly improved mission performance.
- Promote results-based performance measures and best practices to improve mission performance and optimize the return on investment for IT/IM.

1.4.3 Navy Application Database Task Force (NADTF)

The NADTF was established in March 2002 to act as the focal point for the Navy in developing a reliable inventory of legacy software applications. The NADTF was responsible for:

- Overseeing Navy-wide legacy application identification.
- Coordinating (through Program Management Office (PMO) San Diego) the entry of needed application information changes into the ISF Tools Database.
- Identifying the Program of Record (POR)/CDAs for legacy applications.
- Identifying a standard version for the Government Off the Shelf (GOTS) applications.
- Working with the PEO-IT Enterprise Solutions Office and Department of the Navy Chief Information Officer (DON CIO) to identify recommended Commercial Off the Shelf (COTS)

application products and product versions so the Navy could acquire required Enterprise Licenses.

- Working with other Navy groups Legacy Applications Task Force (LATF), the NMCI Program Office, PEO-IT's Enterprise Solution Office (ESO) and TFW to obtain synergy and prevent duplication of efforts. The NADTF reports directly to the Navy IO (OPNAV N-7) and the Director, NMCI to reduce the number of applications that must be integrated into NMCI through:
  - Elimination of inappropriate applications
  - Standardization of application versions
  - Recommending applications be quarantined if the application violates established security parameters,
  - Recommending applications be rejected if media is not available at an appropriate time prior to cutover, and
  - Providing other recommendations that will enhance the ability to roll NMCI seats while weighing the costs versus benefits to the individual commands.

NADTF was established to provide a comprehensive approach for identifying and reducing the number of software applications being used by the Navy. This process was undertaken in cooperation with the NMCI PMO in San Diego and consisted of reviewing the initial application data call that had been entered into the ISF application database, standardizing the naming convention to eliminate duplicate entries, and eliminating applications and application components that could not operate within the established NMCI Windows 2000 environment. Specifically, the Task Force's objectives were to:

- Identify all Navy software applications, whether or not they would be required to run in the NMCI environment,
- Facilitate entry of software application information data into the ISF Tools Database
- Take the lead in standardizing software application terminology (name, version, etc.), including serving as the final authority for establishing the naming convention for all software applications (including version designation)
- Provide recommendations to standardize to a limited number of software versions, which would reduce the number of software applications required to be implemented into the NMCI environment
- Coordinate the efforts of the NMCI Program Office, PEO-IT's Enterprise Solutions Office, PEO-IT's NMCI Office and the LATF to obtain synergy and avoid duplication of effort
- Enhance Navy awareness and knowledge of the NMCI implementation process, and
- Provide regular status reports on progress achieved in reducing the number of legacy applications to the OPNAV and Secretary of the Navy staffs.

As commands commenced the cutover to NMCI the role of the NADTF changed in response to specific problems that were being encountered during seat rollout. Some of the major initiatives that are underway include:

- Identifying the CDA for each GOTS application.
- Identify those software applications that are not on the Gold Disk but are widely used throughout the Navy. The intent is to identify ways the Navy could acquire enterprise licenses to reduce the cost of ownership of these applications for each command and across the enterprise.
- Assist the Navy IO in establishing FAMs. The FAMs will be responsible for identifying those applications in each of 23 functional areas that should be established as "standard applications" for use in the Navy.
- Recommending GOTS and COTS applications (by version) that should be established as standard applications within the Navy.
- Act as the processing authority for software application waiver requests for applications that are identified and submitted late after AOR-60, after the commencement of cutover, and after cutover has completed.
- Refining the NMCI Legacy Application Ruleset for applications. This Ruleset determines the criteria that must be met for an application to be permitted to operate within NMCI.
- Working closely with the NMCI Designated Approval Authority (DAA) to ensure the NMCI security posture is not compromised by non-compliant applications.

As the rollout of NMCI accelerates and the number of NMCI users increase, it is expected that the role of the NADTF will continue to change in response to user demands. As more experience is gained with the NMCI network, policies and procedures will be established to standardize operating procedures across the Navy and begin to address the integration of NMCI with other command and control networks within the Navy.

1.4.4 Functional Area Manager (FAM)

FAMs are responsible for application and database rationalization as described in SECNAVINST 5000.36 (see https://neds.nebt.daps.mil/). FAMs are responsible for enterprise management of applications and databases assigned within their functional areas. FAMs are appointed by OPNAV and are responsible for the following:

- Develop and manage IT application and database portfolios
- Ensure that technology strategies are aligned with business and warfighting strategies.
- Resource the application and database implementation, certification and accreditation (C&A) for applicable Navy networks.
- Fund and manage the introduction of updates and revisions to the applications and/or databases.
- Reduce and consolidate IT applications and databases within their functional area to a preferred products list (PPL).
- Ensure metadata and data elements in use are registered and compatible with designated authoritative databases.

- Migrate or retire quarantined applications and databases.
- Work closely with the DON CIO and the DON Information Executive Committee Service representatives to ensure that common DON processes and procedures are consistently used to accomplish this task.
- Approval authority for POR/CDA to develop an application.
- Work with the PORs and CDAs to develop strategies to retire older, obsolete applications and ensure that only current and recommended applications are in service.
- Identify COTS applications for Enterprise Licensing.
- Standardize to COTS Applications and Version.
- For more information on FAM responsibilities see the NEADG.
- Directed by CNO to reduce Legacy Applications and databases by 95% by May 2003.

The DON CIO is expanding the functionality of the current Department of the Navy Application Database Management System (DADMS) to support the FAM application rationalization process. Each Echelon II command has representatives working closely with the FAM on their applications and databases. Developers and program managers who have questions about the FAM processes should contact their Echelon II Functional Area representative, or the FAM Lead.

1.4.5 Functional Data Manager (FDM)

The FDM is responsible for implementing functional processes to produce and monitor the use of data within and across functional activities, information systems, and computing and communications infrastructures. FDMs are appointed by OPNAV and are responsible for the following:

- Assist program managers and other system developers in registering system/application (metadata) and data exchange formats and maintaining the metadata baseline.
- Develop and maintain Functional Area views of the DON Data Architecture.
- Develop candidate DoD standard data elements in coordination with the respective Functional Data Administrator (FDA).
- Coordinate with applicable stakeholders to ensure DoD proposed Data Standards are useable by DON Systems.
- Designate the Authoritative Data Source (ADS) for their respective functional areas and maintain the designation in the DADMS using processes and procedures approved by the DON CIO.

1.4.6 Naval Network Warfare Command (NETWARCOM)

NETWARCOM is the Navy's central operational authority for space, IT requirements, network, and information operations in support of naval forces afloat and ashore; to operate a secure and interoperable naval network that will enable effects-based operations and innovation.

NETWARCOM coordinates and assesses the Navy operational requirements for and use of network/command and control/IT/information operations and space. It serves as the operational forces' advocate in the development and fielding of IT, information operations and space and to perform such other functions and tasks as may be directed by higher authority.

NETWARCOM are responsible for the following:

- Provide a single source of information support to the fleet through assumption of central responsibility and authority over all aspects of information management.
- Act as the Navy's central authority for space services, IT, network and information operations in support of naval forces afloat and ashore.
- Approval authority for the deployment of all applications into the NMCI environment. In addition, NETWARCOM is responsible for the prioritization and scheduling of applications for submission to ISF.
- Provision a secure and interoperable naval network that will enable effects-based operations and innovation; coordinates and assesses the Navy network/command and control/IT/information operations and space requirements.
- Serve as the central operational authority responsible for coordinating all IT, information operations, and space requirements and operations within the Navy.
- Operate and maintaining the Navy's global IT systems and services, including enterprise networks, through assigned worldwide communications activities and related contracts which support warfighting operations and command and control of naval forces.
- Serve as the single focal point for navy base level communications policy, procedures, and resources; consequently, operation and management of the Navy's Base Level Information Infrastructure (BLII).
- Operate the "Information Technology for the 21st Century" (IT-21), a program designed to upgrade network systems aboard ships.
- Oversee the Navy's computer network attack and defense work through IT-21 and the NMCI procurement with Electronic Data Systems (EDS) Corporation.

1.4.7 NMCI Designated Approval Authority (NDAA)

The DAA is a senior policy official that has responsibility and authority to make the management decision to accept or not accept the security safeguards prescribed for an Automated Information Systems (AIS). The DAA is the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

Responsibilities:

- Establish and promulgate the guidelines and security requirements applicable to the NMCI network and the software, which operates on that network.
- Assure the fulfillment of the system accreditation for his/her organization.
- Ensure that the AIS security mechanisms enforce the security policy of the organization.

1.5 INFORMATION STRIKE FORCE (ISF)

1.5.1 Application Integration and Testing (AIT)

The AIT lab is responsible for packaging and NMCI Certification testing of Enterprise applications, emergent (new) applications, and updates/upgrades/patches/fixes for existing applications. CDAs or an ISF Site Team (Site Solution Engineering Base Lead or Site Transition Manager) are responsible for providing media to the AIT for packaging. AIT is responsible for these functions and responsibilities at the San Diego Certification Lab, the Classified Lab at the San Diego NOC and the Complex Application Laboratory (CAL).

Once an application has been packaged (either in the lab/NOC or at the site), the AIT then certifies the package for deployment via Radia. If the package passes Certification, it is placed on the Radia servers for distribution to each of the NOCs. The package will later be tested on-site during Legacy Application Deployment Readiness Activity (LADRA).

AIT Responsibilities include:

- Auditing of applications for compliance with the NMCI Rule Set Packaging of applications for deployment
- Certification of applications for deployment
- Deploying package to the Novadigm Radia Servers

1.5.2 Site Manager (SM)

The ISF SM is the lead ISF NMCI member at each site. The SM is responsible for the delivery of all NMCI services at the designated location. Service delivery roles include:

- "As-is" support during the Assumption of Responsibility (AOR) period
- Migration / transition support during the cutover period
- Post cutover daily production support of existing and new Navy requirements
- Coordinate ISF operations for the site

1.6 CLAIMANT

1.6.1 Sponsoring Echelon II Command

An Echelon II Command or claimant is defined as an activity that reports to CNO or higher as a normal part of operations. The Echelon II Command is responsible for exercising application management over all subordinate units or organizations. The Sponsoring Echelon II Command is defined as the parent organization of the POR and CDA. As the parent organization the Sponsoring Echelon II Command provides program and content oversight of the applications and releases. The Sponsoring Echelon II Command plays a review and approval role in the Release Deployment Process.

1.6.2 Program of Record (POR)

The POR is an office or individual who sponsors and has ownership responsibilities for an application. These responsibilities include but are not limited to funding and maintaining the application. The POR will conduct periodic reviews of their applications to determine if the application is current or requires a more detailed review and update. The POR in conjunction with the CDAs and FAMs must develop a strategy to retire older, obsolete applications and conduct periodic reviews to ensure that only current applications are in service.

1.6.3 Central Design Authority (CDA)

For the purposes of this guide, a CDA is anyone (any organization, site, group, department, division, unit, section, or individual), government or government sponsored contractor, who desires to introduce a new application or change to an existing application within NMCI environment. CDAs are responsible for ensuring that their releases are compliant with Navy IA, boundary, and GPO policies prior to deployment within NMCI. CDAs must work with the PORs and FAMs to develop strategies to retire older, obsolete applications and ensure that only current applications are in service. CDAs must keep in mind the requirements for developing and migrating applications that comply with TFW, NMCI, IT-21, Outside-Continental United States (OCONUS) BLII architectures, and DON standards.

CDAs are also known as Central Design Activity, Central Development Activity, or Commercial Design Activity. All of these terms are synonymous as used in this document.

1.7 LEGACY APPLICATIONS

As defined by the NMCI Contract, a legacy application is “An existing customer software application that is not included in the NMCI standard seat services or the Contract Line Item Number (CLIN) 0023 catalog.” Applications are in use today at sites by people performing the mission or business of the DON. Legacy applications are NOT part of the standard seat services (also known as Gold Disk) provided by the ISF. For more information associated with migration of Legacy Applications to NMCI and the latest information on the ISF certification process, please refer to the LATG at http://www.nmci-isf.com/legacy_applications_transition_guide.pdf .

1.8 TRAINING

POR/CDAs are responsible and must plan for preparing, conducting and funding any training necessary to support their release. Training should coincide with the release deployment phase and be included in the Release Deployment Plan (RDP). Training should also address the potential impact the release may have within NMCI. The details of release training and the training plan are the responsibility of the POR/CDA and their Sponsoring Echelon II Command. This guide does not provide the details of the training requirements and training plan. See Appendix G for the Release Deployment Plan.

Note: *New release training is not a responsibility of the ISF.*

1.9 NMCI INFRASTRUCTURE ARCHITECTURE

This section follows the organization of *Figure 1-1*, Architecture Management Framework.

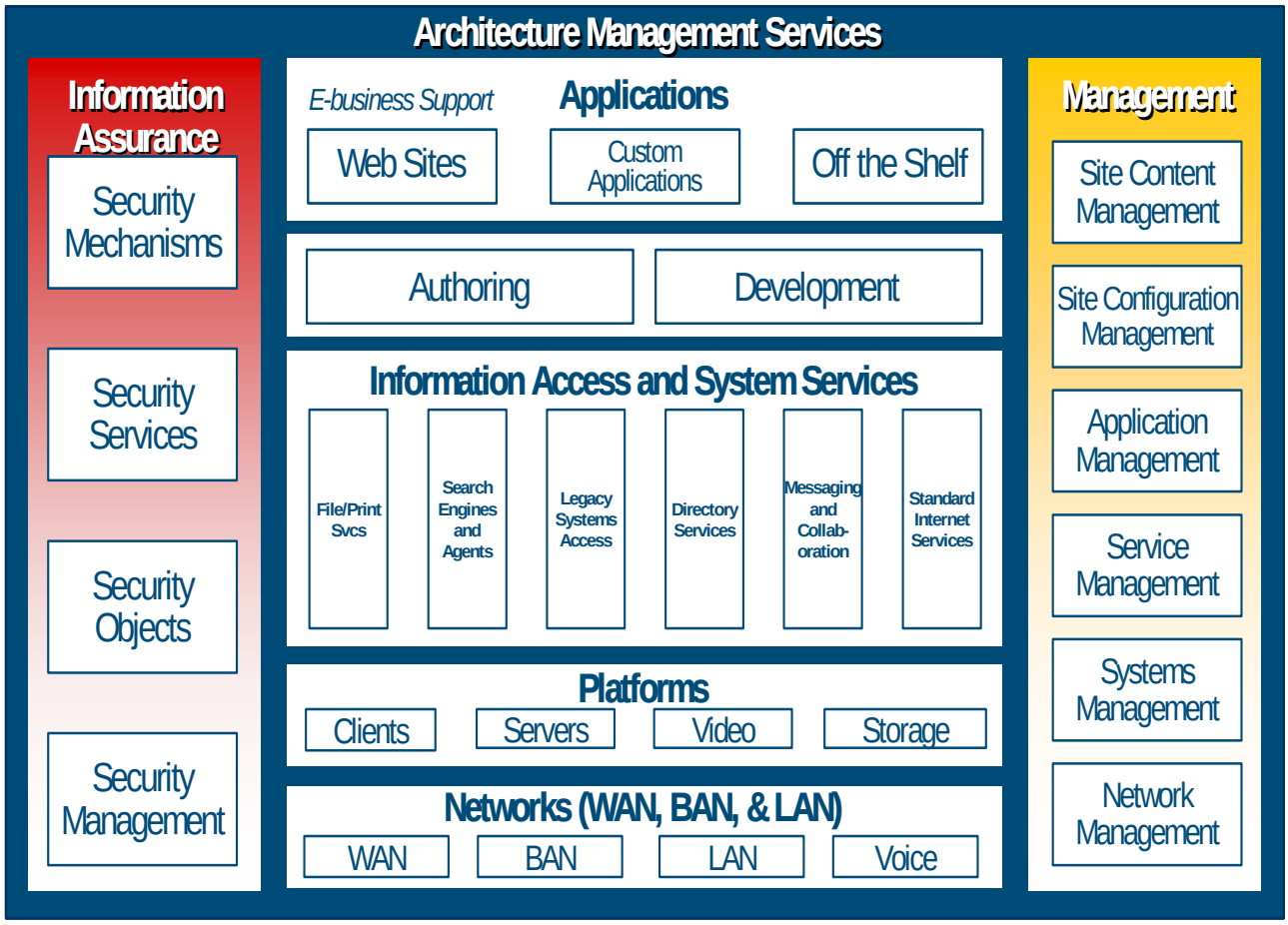


Figure 1-1 Architecture Management Framework

This figure details the overall design components of the NMCI architecture and shows the technical application requirements as well as logical and physical architectures. Architecture information is presented by subcomponent and includes conceptual issues and items relating to security, management functionality, and deployment

2.0 NMCI APPLICATION RELEASE CYCLE

This section describes the policy, procedures and processes that a CDA must follow in order to obtain authorization to introduce an emerging application or develop a release that supports an existing NMCI application. These procedures and processes are currently being developed by the NMCI Application Release Management Working Group (NARMWG) and will be incorporated into the guide when available. Current information on these processes is presented to provide a basic understanding of the conceptual approach to release management.

The slide below depicts the overall process of the NMCI Application Release Cycle that supports the management process and the introduction of an emerging application into NMCI. The processes indicated in the ***beige*** colored boxes are covered in greater detail in Chapter 5 of this guide with the exception of Operations. The ***blue*** colored boxes are discussed in greater detail in the following paragraphs. When applicable, those functions that **do not** have business processes will be identified and that information will be incorporated into the guide when available.

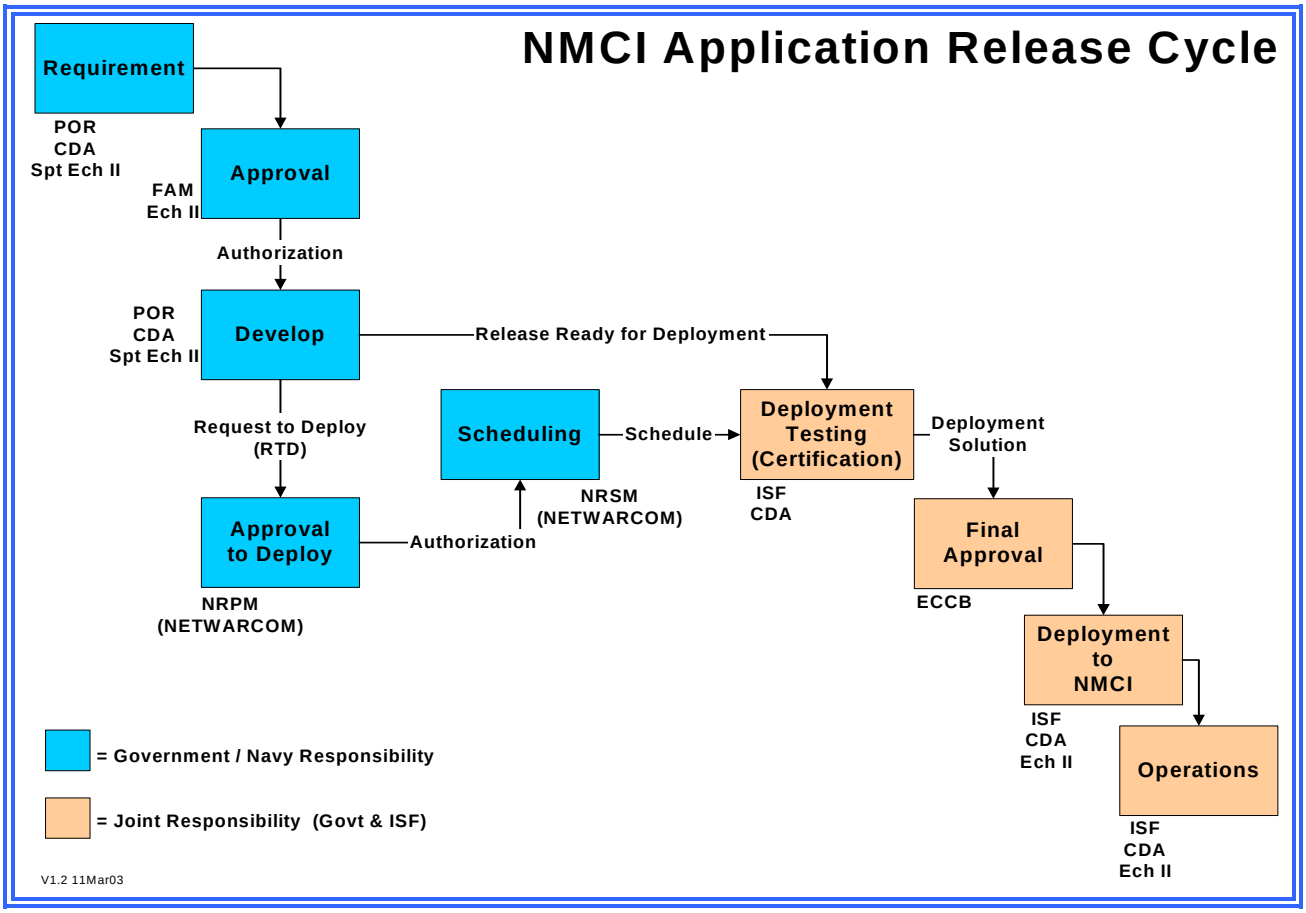


Figure 2-1 NMCI Application Release Cycle

2.1 REQUIREMENT DETERMINATION

This is the responsibility of the customer in making the determination for the sustainment of an existing application or the introduction of an entirely new application. Introduction of new applications may include the deployment of an application that is currently certified and deployed within NMCI to a new site.

2.2 APPROVAL

The Functional Area Manager (FAM) is the designated approval granting authority for the development of applications and releases that will operate within NMCI. The CDA must be granted approval prior to beginning work on the development of an application or release, this also includes the introduction of an emerging application that has previously been developed. POR/CDAs must contact their appropriate FAM to determine the approval requirements for their release.

2.3 DEVELOPMENT

FAM approval is authorization for the CDA to proceed with the development of the application or release. Once the CDA has completed development, has performed and satisfied all pre-certification testing requirements as discussed in Chapter 5 of this guide, a Request To Deploy (RTD) will be submitted to NETWARCOM for approval to deploy the release. Since it is possible for numerous months or years to elapse between the authorization to develop and the actual deployment of the release, it becomes necessary to execute a separate request and approval process for deployment. The RTD form can be found in Appendix J of this guide.

2.4 APPROVAL TO DEPLOY AND PRIORITIZATION

Commander, NETWARCOM is the approval authority for the deployment of releases in NMCI. The business processes to support this function require development and integration within the overall release management process. NETWARCOM will review all RTDs, take action to approve or disapprove the deployment request.

Additionally, the Commander, NETWARCOM has the responsibility for establishing release prioritization. Once approved the request will be reviewed for its significance and priority in release deployment timing. This includes review and approval of all requests for Unplanned Emergency/Urgent releases.

Documentation prepared by the CDA must provide sufficient information regarding the release to enable NETWARCOM to establish prioritization. Information to support prioritization of a release will be sourced from the FAM approval document and the RTD.

NETWARCOM will establish a subordinate activity to support this process; the NMCI Release Prioritization Manager (NRPM) is responsible for ensuring that each release is properly prioritized prior to submission into the scheduling process.

Prioritization decisions will be based on criteria that include required deployment date for the application, if applicable. Some of the criteria for the determination of prioritization are based on the following requirements/mandates (this is not all inclusive list nor in any particular order):

- Safety
- Fiscal – Changes that effect military, civilian, and contractor pay
- Security - Information Assurance Vulnerability Alert (IAVA)
- Operational
- Legal (Requirement or Obligation)
- Congressional – Congressional recording requirements / Budgets
- Ongoing war efforts
- Treaty with a Sovereign Nation (i.e. Status of Forces Agreement (SOFA))
- Department of Defense
- Department of the Navy
- Local Commander
- Major systems
- Minor systems

2.5 SCHEDULING

Commander, NETWARCOM is the activity for scheduling all release submissions to ISF. The business processes to support this function require development and integration within the overall release management process. To properly support and manage the throughput of releases submitted to the ISF, NETWARCOM will establish a subordinate activity to support this process. The NMCI Release Scheduling Manager (NRSM) is responsible for scheduling releases for submission to ISF and is the interface between the CDA and ISF. The NRSM is responsible for the following:

- Develop release submissions schedules with the ISF
  - First-In-First-Out (FIFO) rule
  - Enforce release priorities directed by the NRPM
  - Emergency/Urgent consideration
- Distribute schedules
- Work with ISF and CDAs to resolve scheduling conflicts
- Maintain processing oversight for all releases

2.6 GOVERNMENT PREDEPLOYMENT COORDINATION

The POR/CDA, Echelon II, site/command and any others as needed, coordinate the approved request and monitor deployment of the application/release. This coordination is the joint

responsibility of the appropriate POR/CDA and Echelon II. It will ensure that all necessary deployment requirements, elements, and issues are addressed and resolved. Such as notification, scheduling, testing, setup, configuration, mapping, etc.

2.7 USER TO APPLICATION MAPPING (UTAM)

A deliverable of the POR/CDA, Echelon II, and site/command deployment coordination step is a functional User to Application Mapping (UTAM) plan for deployment of the application/ release at each location. The preferred method for completing the UTAM is utilizing the Navy Ordering Interface System (NOIS). If NOIS is not available the UTAM can be completed using the spreadsheet form depicted in Appendix I. The UTAM will be submitted to the ISF for use in deployment of the application/release.

2.8 APPLICATION DEPLOYMENT

Once all pre-deployment steps and requirements have been met, the ISF will begin deployment of the application/release at the appropriate locations in accordance with the coordinated schedule, UTAM, and other requirements. Deployment of the application/release is the responsibility of the ISF. Depending on contractual language and requirements, the site/command maybe responsible for providing one Move, Add, Change (MAC) request for deployment of the application/release at each site.

2.9 OPERATIONS

Operations deals with the sustained state of the application/release, after it has been deployed. Operations is beyond the scope of this guide.

3.0 PREPARATION AND ANALYSIS PHASE I

This phase is designed to provide the developer with an overview of DON policies and NMCI requirements that must be considered in the development of new applications or changes to existing applications. Applying this information during the design and development phase will reduce delays in getting applications through the certification, accreditation, and deployment processes.

3.1 DATA COLLECTION AND ASSESSMENT

Under the control of the DON CIO, a database catalogue has been created to list all current applications that reside on the ISF Tools database. It is the responsibility of the FAMs and POR to provide to the developer of new or emerging applications the ability to review this data. Further, it is the responsibility of the developers to conduct an analysis of this data to ensure either there is no duplication of capabilities, or that the new or emerging application will operate properly in the NMCI Environment. Appendix E contains a list of factors to be used for evaluation of applications migrating into NMCI. Furthermore, it is the responsibility of developers to obtain FAM approval prior to proceeding with development.

3.2 ENTERPRISE RATIONALIZATION

Enterprise Rationalization is the process of identifying only those desktop and server-based applications, both COTS and GOTS, required to support command or DON missions, goals, and business processes. It includes the integration, consolidation, and elimination of applications and associated databases to improve standardization, enhance security, reduce duplication, and minimize support costs. Not all applications need be targeted for NMCI. Rationalization policy and guidance is the responsibility of the DON CIO. Service-level policy and guidance for rationalization is the responsibility of respective Service CIO. Claimant/Marine Corps-level policy and guidance for rationalization of software applications is the responsibility of the CIO of the claimancy/Marine Corps organization.

The DON-level enterprise rationalization process is a structured approach to an information management framework. This includes functional and acquisition program managers to ensure horizontal integration (HI) of systems and databases and will tie into the Enterprise Resource Planning and TFW initiatives. This effort includes identifying duplicative applications, older versions of applications, applications that have already been certified, and working with the Navy claimants and Marine Corps organizations to resolve these issues. The FAMs will lead this rationalization process.

3.3 DON APPLICATION AND DATABASE MANAGEMENT SYSTEM (DADMS)

DADMS was created to provide a tool to the FAMS that would enable them to segregate application by function, identify and catalogue application attributes, and manipulate information related to application to facilitate the reduction of applications to a minimum number needed to support the operation of the Navy IT enterprise. To enhance the Navy's success in effectively implementing NMCI, the CNO has established a goal to reduce Navy Legacy Applications by 95

percent within one year or by May 2003. To accomplish this effort the DON CIO has directed the development of the DADMS to support the FAMs and FDMs in developing standard applications, databases, and data elements and provide the structure to maintain configuration control of all applications and databases across all DON networks. This will facilitate the integration process to capture both the Navy and Marine Corps existing IT business rules and requirements. The processes and procedures can be found on the DADMS website under policy and guidance link.

3.4 PROCESS FOR RATIONALIZATION

The purpose of these processes is to reduce the number of redundant or obsolete applications and corresponding databases with in a functional area (business process) and optimize the configuration of IT. All applications (COTS and GOTS) in the DON will belong to a FAM for enterprise application management. It is the responsibility of the FAM to ensure that their applications have been rationalized and are managed in accordance with all applicable directives and guidance. This will ensure validity of all applications within the enterprise. This process must be accomplished prior to the development of any new application or changes to existing applications. The rationalization of COTS and GOTS applications begins with FAM interaction to determine if the application is a DoD or DON-standard application.

The actual details of the enterprise rationalization process are beyond the scope of this guide. Detailed information on the rationalization process is addressed in the LATG and the DADMS website under policy and guidance.

3.5 NMCI Application Ruleset

All applications will be reviewed against the NMCI Ruleset for compliance. Applications that are found not in compliance with the Ruleset are subject to NAVY IO waiver or are Killed and removed from NMCI. Not all Rulesets are waiverable and not all will set violations result in a Kill. More detailed explanation of the Ruleset requirements can be found in Appendix D.

Request for waivers for applications that violate these rules will be submitted by the responsible Echelon II command to the Navy IO Attn: NADTF. NADTF will adjudicate all waiver requests, for the NADTF Waiver Process refers to paragraph 3.6 below.

The following rules apply to GOTS and COTS applications within NMCI:

1. Windows 2000 (W2K) Compatible
2. NMCI Group Policy Object (GPO) Compatible
3. No Duplication of Gold Disk Software or Services
4. Comply with DON/NMCI Boundary 1 and 2 Policies
5. No Setup, Installation, Uninstallation, Update and Auto Update Tools or Utilities
6. No Games
7. No Freeware or Shareware

8. No Beta/Test Software (Authorized on S&T Seats Only)
9. No Application Development Software (Authorized for S&T Seats Only)
10. No Agent Software.
11. Gold Disk Compatible
12. No Peripherals, Peripheral Drivers or Internal Hardware
13. No personal, non-mission, or non-business related software
14. No 8/16-Bit Applications

For a description and more details on the Ruleset, go to Appendix D.

Other applicable rules may emerge from the DON or the Echelon II command.

In addition to the above rules, CDAs are encouraged to consider development requirements specific to supporting IT-21, the Marine Corps Tactical Network (MCTN), BLII and the TFW. The goal is to standardize application and databases across all networks, if feasible.

3.6 NADTF WAIVER PROCESS

The NADTF has developed an NMCI Waiver Request Submission Guide to provide clear guidance for submitting NMCI Application Late Application/Change Waivers to Navy IO (NADTF). Each Echelon II command shall have a POC to manage the application and change process, and this includes the resources to submit and manage waivers for all subordinate commands per the NAVY IO Guidance. The purpose of the NRD²G is to provide guidance in the development of a release to eliminate the need for a waiver; however there may be a requirement for a waiver based on the status of the parent application being supported. It is critical that each CDA understand all requirements outlined in the references provided, and work with their assigned Echelon II POC to ensure all waiver requests contain complete and accurate information and are in the required format. The Waiver Input Template (WIT), as outlined in the link below, has been developed to improve accuracy and reduce duplication of effort on the part of the waiver requestor and the Navy IO (NADTF).

The current version of the guide can be obtained through the NADTF website at: http://cno-n6.hq.navy.mil/NaVCiO/leg_apps.html

3.7 INFORMATION ASSURANCE (IA)

IA is critical to the success of NMCI. Through technical protections and procedures, NMCI enables its users to access information and services with the trust necessary to do their jobs. Defense-in-depth protection mechanisms are deployed in a layered fashion forming boundaries at multiple levels within the security architecture. This process ensures resistance to attacks and minimizes the possibility of a security breach due to a weakness (known or unknown) at any single security component. The defense-in-depth protection strategy provides security features to NMCI systems and data. These features are confidentiality, integrity, availability, accountability,

authentication and non-repudiation. Elements comprising various aspects of IA provide the above listed security features.

3.8 SECURITY

3.8.1 Boundary Protection

A standard set of protections has been incorporated into NMCI to protect the interfaces within NMCI and between NMCI and other networks. The framework, for these protection standards, is provided in the NSA Guide to Securing Microsoft Windows 2000 Networks, as published by the Network Security Evaluations and Tools Division of the Systems and Network Attack Center (SNAC). See *Figure 3-2*. Boundary Protections enforce the policies required to connect to external networks, provide security mechanisms for secure access to applications, and protect Communities of Interest (COI) residing within NMCI. This area is discussed in greater detail in Phase II of this guide.

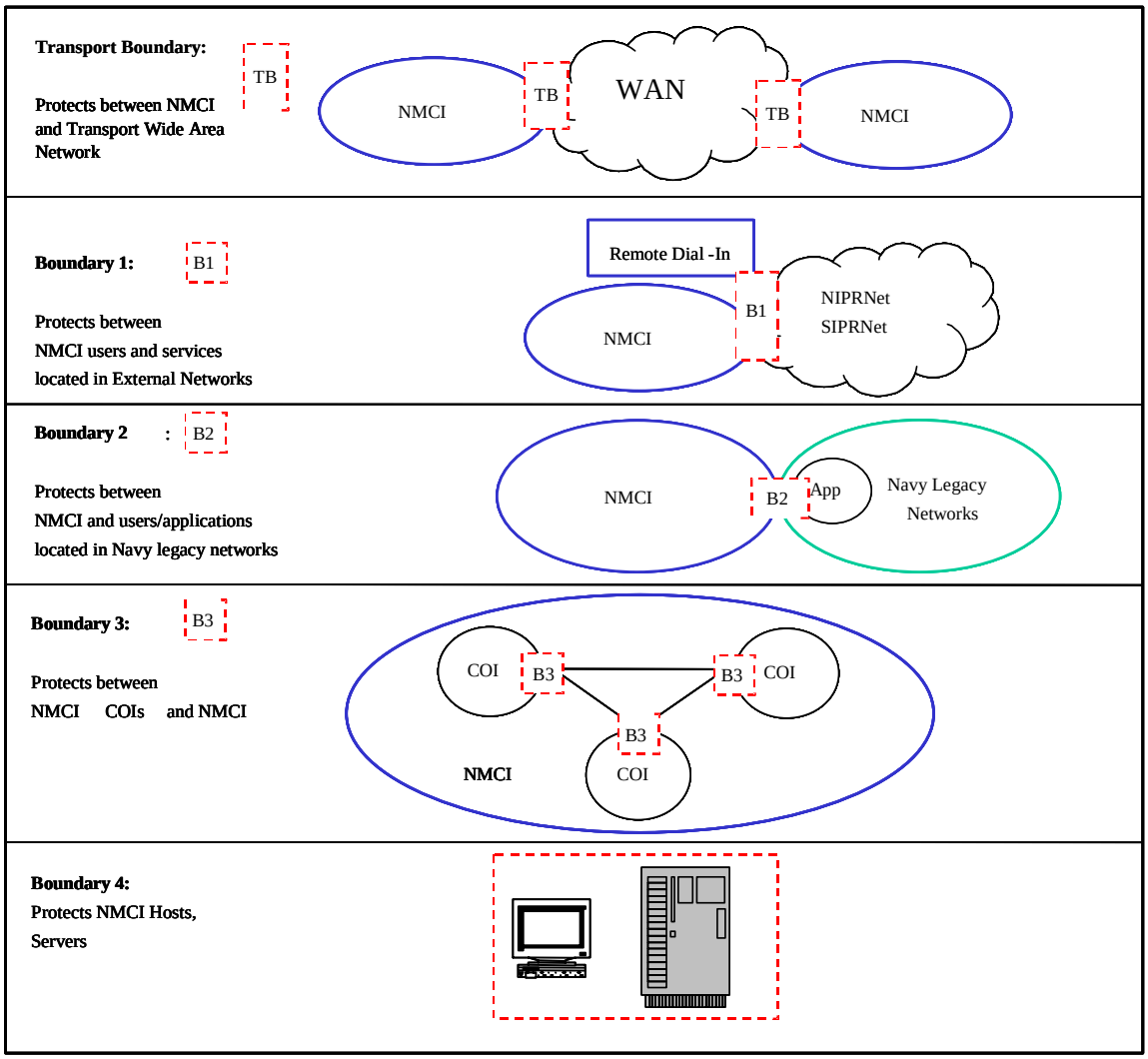


Figure 3-1 Network Boundaries

3.8.2 NMCI Public Key Infrastructure & Directory System

NMCI employs Public Key Infrastructure (PKI) Class 3 certificates for strong user identification and authentication (I&A) and e-mail signing. NMCI infrastructure components are Public Key Enabled (PKE) to authenticate to each other. The NMCI implementation of DoD PKI provides accountability and non-repudiation, and to a lesser degree, data confidentiality and integrity.

One of the most common issues that prevent integration of content into NMCI is compliance with boundary and GPO policies. NMCI is compliant with DoD and DON security policies using 2-way Secure Socket Layer (SSL) and will require the installation of a DoD Class 3 PKI identity certificate. Users must contact their local certification authority to obtain their PKI certificate. Specific DoD implementation of PKI in the Navy can be found at the InfoSec website's PKI primer at https://infosec.navy.mil.

3.8.3 Boundary 1 (B1) Conditionally Allowed Ports

There are typically "Conditions" attached to the use of these ports that are "Conditionally—Allowed" on NMCI. All applications that must communicate over the "Conditionally Allowed" ports must adhere to the "conditions." If proper compliance to the "conditions" is achieved, the application is permitted on NMCI (from an operational perspective). That is, the CDA doe not have to submit a "Request to Operate A Non-Compliant System" to Space and Naval Warfare Systems Command (SPAWAR) PMW-161 for processing through CNO.

Site/commands or POR/CDAs must provide sufficient information to the DAA that the application/release will comply with the "conditions" and ensure the ISF B1 Firewall administrators understand the conditions. Each application that will attempt to use the "Conditionally-Allowed" port must have the following information submitted in order to receive authorization to deploy the application:

- DoD Information Technology Security C&A Process (DITSCAP)/5239 based System Security Authorization Agreement (SSAA) Package
- Interim Authority To Operate (IATO) letter of recommendation issued by SPAWAR PMW-161 for large Program of Record
- POR, or NETWARCOM or local/CDA DAA for smaller systems (non-POR)
- If an IATO already exists, the IATO must be submitted to NETWARCOM for review along with the SSAA package.
- The total port, protocol, service, and direction of initiation (P/P/S/DI) requirement for system communications and topology are required. Destination Internet Protocol (IP) Addresses will be required for specific port usage.

For each Legacy Application/System transitioning to NMCI and using the "Conditionally-Allowed" ports, the NMCI DAA/NETWARCOM will maintain a listing/ registry to ensure they have a complete picture of which ports are being used. This listing will support enterprise decisions for IAVA's, NAVCIRT Advisories, etc.

3.8.4 Security Services

Within NMCI, security administration uses the basic features of the Active Directory (AD), Groups, and Organizational Units (OU). AD is Microsoft's trademarked directory service (DS) that provides the basic security policy enforcement and access control administration mechanism for NMCI.

3.8.5 Security Objects (Group Policy Objects)

The security mechanism for Windows 2000 AD is the GPO. NMCI Group Policy Operational Guidelines will not be published in this guide but are available to CDAs through the NMCI Enterprise Applications Group for Legacy and Emerging (EAGLE) Team Facilitator. This area is discussed in greater detail in Section 4.4, of this document.

3.8.6 Security Management

DON and ISF personnel manage NMCI security jointly. DON sets policy and the ISF is responsible for implementation. Although the Security Operations Centers (SOCs) will be staffed primarily with ISF personnel, the DON exercises Command Authority over DON defensive Information Warfare activities. Security is managed in compliance with all relevant DoD and DON policies.

3.8.7 Firewall Policies

CDAs can access the complete non-classified Navy Fleet Firewall Policy (FFP) and the USMC non-classified Firewall Policy at the following URL: https://infosec.navy.mil.

3.8.8 Desktop GPO Implementation

NMCI is enforcing Navy and Marine Corps security policies by using AD services and GPO policies. Application installation, configuration and updates are handled by the ISF using Novadigm Radia packages. NMCI users will not be permitted to install software, except on a Science and Technology (S&T) seat. Novadigm Radia packages include settings in configuration files, set path variables, icon file location, application drivers, etc. If the release settings violate GPO policy, the CDA will be required to reconfigure the release to comply with policy requirements.

3.8.9 File and Registry Permission – Description

NMCI client images contain file and registry permissions designed to conform to security requirements while allowing most applications to function properly. Following is a description of how these settings affect applications deployed to NMCI clients.

3.8.9.1 File Permissions

The NMCI client image has special file permissions. The NMCI user desktop is a single partitioned C drive. The GPO only allows users and applications to create subdirectories and files in designated areas of the file structure:

- NMCI Desktops are set with the NMCI ISF screen saver. The screen saver cannot be changed.
- Users can create subdirectories in the root directory.
- Applications can create subdirectories in the C:\PROGRAM FILES directory during installation.
- All operating system level files (autoexec.bat, System32, etc.) are not available for update by applications. The C:\WINNT directory can be written to or appended, but not overwritten.
- Desktop users are not allowed to make changes to application files. Application files are distributed to the user's desktop using AD, Novadigm Radia, and Gold Disk processes.

It is required that releases deployed to NMCI clients be placed in subdirectories below C:\PROGRAM FILES. NMCI requires that release data be stored in the user's "My Documents" subdirectory. The location of the "My Documents" subdirectory should be obtained programmatically because this will not be the same for all users / profiles – for example Terminal Services users have their My Documents subdirectories re-directed to their home subdirectories on the network. The location of subdirectories is defined in the following registry key: http://www.microsoft.com/windows2000/techinfo/howitworks/default.asp

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal

The location can also be obtained using the following Visual Basic, C/C++ function:

SHGetFolderPath (NULL, CSIDL_PERSONAL, NULL, 0, szPath);

To ensure that NMCI workstations are both secure and stable, users (and applications) are allowed to write in only designated directories on their local hard drive. These permissions are enforced using the Windows 2000 GPO.

3.8.9.2 Registry Permissions

Registry permissions change periodically. For current registry permissions refer to the GPO information provided by the NMCI EAGLE Team facilitator. As with file permissions, Radia can write to all areas of the registry during installation of the application via the system account. However, once the application is installed, the user is restricted to the areas governed by the GPO while running the application. Therefore, the application should be designed to only write to those areas during runtime.

3.9 INFORMATION ACCESS & SYSTEM SERVICES

3.9.1 File & Print Services

File and print services are two of the most fundamental services within NMCI. File servers provide secure storage space for both public and private files. Print services allow users to produce black and white, color, or transparent hard copies of work created with NMCI hardware and software. Both services rely on the server platform and are connected to the user through the physical networks.

User Identification and Access. It is important to limit server access to users who are known and approved. This is accomplished using Windows 2000 user access technologies. In some cases certificates are used to identify users. If a user is not capable of clearing the authentication process, they are not granted access to the file or print solutions.

Computer Virus Protection. NMCI defense in depth provides for virus monitoring at several points within the NMCI architecture. Virus definition, OS patches, and other updates occur automatically. Computer systems must be left on overnight, with the user logged off, for network managed software housekeeping to occur.

3.9.2 Print Services

The Windows 2000 print subsystem as managed by AD allows a user to query the AD for available printers, in addition to the default printer. Developers will use AD to determine that a printer has the required print capabilities.

3.9.3 File Storage Services

Each NMCI user account is allocated one gigabyte of storage on a file server. This storage space is designated as private storage, public storage, or growth area. Public storage is pooled and controlled at the Command level. Additional public storage can be purchased in ten-gigabyte increments by requesting a Task Order (TO) under CLIN 0016. The 1000 MB of user storage space is divided as follows:

- 700 MB private
- 100 MB public
- 200 MB (25% growth)

The following drive letters and backup routines are available:

Drive	Description	Incremental	Full Backup	Shared
C:	My Documents - local desktop. GPO rules are applied	None	None	No
H:	(Home) network directory for a user's private	Nightly	Weekly	No
S:	(Shared) network directory Command's public	Nightly	Weekly	Yes

Users do not have delete or change permissions and cannot take ownership of files they did not create. Users are not allowed to share private storage or create shares on their desktops. Developers must not re-map the public (S) and private (H) network directories. Users should verify that adequate space is available on a network drive before writing files to these resources.

3.9.4 File Sharing

The ISF implements login scripts to map file shares. Each NMCI user has the H: and S: drives mapped on their machine through a login script. The H: drive is the private drive of the user and cannot be shared. The only file sharing exists on the S: drive and that file sharing is limited to that public portions assigned to that specific user. The standard Microsoft file sharing rules and permissions apply. The C: drive and all of its contents are not shareable. This provides standardization throughout the NMCI environment. Additional shares should be mapped with a drive letter that is consistent across the NMCI enterprise.

3.9.5 Personal Storage

Individuals are assigned a network drive that points to their private data (H:\). They cannot provide shared access to others. Users are given basic file permissions (read, write, etc.) but are not allowed to share. If users wish to share files with others, they must use the Command shared directory space (S:\).

The home drive (H:\) points to a user's personal file space located under the USERS directory on each file server. This space stores files used only by the individual user [for example, files such as the mail personal storage (.pst) file]. Each user directory is shared and full control permissions are given to the user. No other users are given access through the share and the user cannot create additional shares to allow others access. The directory is limited to a maximum of 700 megabytes of disk space (assuming CLIN 0016 was not used to increase the space).

3.9.6 Shared Storage

Within NMCI, shared storage is allocated by Command. Folders and files located in this shared storage permit users to read, write and execute files. Users may create and delete subfolders. Designated individuals within the Command may control access to the shared storage. NMCI shared storage is not accessible from outside the NMCI enclave.

The shared drive (S:\) points to group data. Each Command is given a subdirectory containing the shared space for all of its users. The directory is shared at the Command level and the Command designates which user accounts are made owners of the directory. By allowing the designated owner to control access using NTFS permissions, the Command can exercise the greatest level of flexibility over the allocation of this storage space.

3.9.7 File Share Naming Convention

File sharing will follow standard Universal Naming Convention (UNC) paths. AD uses the following format for file share naming:

\\CCCCCC\LLLL\SSSSSSSSS

Symbol	Represents	Character Count
CCCCCC	Command	Variable
LLLL (Optional) (Local Shares Only)	Site Identifier	Four
SSSSSSSS	Share Name	Variable

File Share naming examples:
\\SPAWAR\SPOT\Group161
\\MARFORPAC\PLMS\SOFTWARE
\\NAVAIR\PAXR\ADMIRALS SHARE

3.9.8 Printer Naming Format

Printers may be up to 80 characters in length. The standard NMCI printer driver is Postscript. AD uses the following format for network printers:

\\LLLL\BBBBBB\FF\RRRR\OOOOOO

Symbol	Represents	Character Count
LLLL	Site Identifier	Four
BBBBBB	Building Identifier	Variable
FF	Floor Identifier	Variable
RRRR	Room Identifier	Variable
OOOOOO (Optional)	Printer Identifier	Variable

Printer naming examples:
\\PAXR\Bld6\02\28\HPLJ5
\\FALL\B421\01\02\HPLJ5
\\MRMR\BLD5\01\331\HPDJ740

3.9.9 Messaging & Collaboration

NMCI messaging uses the Microsoft Exchange 2000 suite. Employment of the system services of this suite will be as follows.

3.9.10 E-Mail Addressing

User Principal Name (UPN): E-mail addresses within NMCI use the (UPN) format that follows the publicly accepted SMTP format. A UPN is a multi-valued attribute of each user object that the system administrator can set. A UPN allows the underlying domain structure and complexity to be hidden from users. For consistency, the UPN and SMTP addresses are the same.

The UPN is unique across NMCI. The naming convention has been adopted as follows:

Firstname.lastname@service.mil (where service represents Navy or USMC)

In the case of multiple users with the same first and last names, the following additional conventions are used to establish uniqueness in the following order of precedence:

Firstname.m.lastname@service.mil where m represents middle initial
Firstname.m.lastname#@service.mil where # represents a unique numeric identifier starting at 1.

Examples of UPNs for several Joe Users who are:
joe.user@navy.mil
joseph.user@usmc.mil
joe.k.user@navy.mil
joe.k.user1@usmc.mil
joe.k.user2@usmc.mil

3.9.11 Mail-Enabled Public Folders

To allow multiple users to access a common mailbox, mail-enabled public folders have been implemented. These folders appear in the global address list as a mail recipient for the Outlook clients. Users that require access to a common mailbox are granted the appropriate e-mail permissions (view, send as, etc.). See Appendix B, Microsoft Developers References for a link to the Microsoft site for the Microsoft Exchange Developers Reference. Developers should be cautioned that not all features are available within the NMCI security model. Developers must understand the restrictions implied by Group Policy and Lockdown to determine which features are available.

3.10 PLATFORMS

3.10.1 Client Seat

The NMCI client seats are ISF-managed seats. Therefore, users do not have administrative rights to desktop configuration or software installation. The basic client seat is delivered loaded with the standard Gold Disk configuration. Additional components can be installed on a client, but these are pushed to the desktop by an administrative facility. As a user cannot add software to his or her seat, it is important for content developers to verify that client plug-ins and components are available and compatible.

3.10.2 Science and Technology (S&T) Seat

This seat upgrade accommodates the special requirements of the S&T community by allowing the hardware and software to be reconfigured by the end user without ISF intervention. This seat will employ architectures and policies that are in accordance with the NMCI ISF security requirements. Customer support will be limited to those services offered by the ISF and not extend to software or hardware loaded and configured by the user. The ISF will not be responsible for SLA performance directly impacted by these seats due to the associated relaxed configuration management (CM) policies. The S&T desktop provides the latitude for those who need a software development platform and the ability to access settings and file locations that are restricted on normal NMCI seats. To order an S&T seat refer to CLIN 0038AA-AH. The S&T seats provide the following:

- Ability to rapidly reconfigure hardware
- Ability to work collaboratively and share data files
- Ability to personally load software to the desktop
- Connect to non-WIN2K Operating Systems (Solaris V8)
- Support non-standard protocols
- High bandwidth requirements
- Appropriate security mechanisms.

Further information of S&T Seats can be found at http://www.nmci-isf.com/userinfo_sandtguide.htm. A detailed description of the CLIN list can be found on the ISF web site at http://www.nmci-isf.com/clinlist.htm.

3.10.3 Simple vs. Complex Developer Applications

Once the application has been categorized to be a development tool, then it must be determined if it is a simple or complex application. A simple application is defined as a standalone application that requires installation on an NMCI workstation only, and has minimal to no dependency on network connectivity to function. The requirement for these applications to use the network for fileshare and network printer requirements does not make them complex. For example, most word processing applications are considered simple applications.

Applications that require network connectivity for standard operation are, for the purposes of this program, defined as complex applications. Any applications that have a separate client side and server side and require network connectivity to be fully functional are considered complex. Server based and client/server applications are examples of complex applications. See the section regarding this type of NMCI Seat.

If the software development application is categorized as simple it will be removed from the ISF Tools Database List and no further tracking/testing by the ISF. If the software development application is categorized as complex he ISF will require evaluation and testing to determine the

application impact on the network. Thus, it must be tracked in the ISF Tools Database and appear on the command's/site's Legacy Application Rationalize List.

3.11 NMCI APPLICATION SERVICES

This section describes services available to developers as part of NMCI. Additional development services may be added over time. This guide will be updated as services are added.

3.11.1 Gold Disk

The NMCI Gold Disk contains standard desktop products and services to be installed on every NMCI client machine. Contents of the Gold Disk will change as NMCI evolves and updates to the Gold Disk build are managed through the NMCI Change Control Process. All releases must be compliant with Gold Disk applications. The following link provides a review of the latest Gold Disk contents: http://www.nmci-isf.com/Gold_disk_contents_11.doc.

3.11.2 Services Available and Unavailable to Developers of Applications

This section is subject to change with the introduction of CLIN 0038AA-AH, for development environments.

3.12 COMPONENTS

Components are reusable programs that can be used as building blocks with other components to provide common services when building an application. Only standard Windows 2000 professional components are provided in the NMCI Gold Disk.

3.12 DIRECTORY AND REGISTRY PERMISSIONS

Releases must be written in accordance with Microsoft Window 2000 standards to ensure compliance with Navy certification standards. In some cases the DON will establish specific permission standards that must also be included in the release. Information on Microsoft directory and registry permissions is available at http://www.microsoft.com/windows2000/techinfo/howitworks/default.asp. For information on Navy/Marine Corps specific permissions contact the NMCI Help Desk.

3.13 BROWSERS

3.13.1 Microsoft Internet Explorer Version 5.0 or Greater

Plug-Ins Provided on Gold Disk. The current set of plug-ins provided by the Gold Disk is shown in the Gold Disk found at: http://www.nmci-isf.com/Gold_disk_contents_11.doc.

The ISF is evaluating additional plug-ins for inclusion in the NMCI Gold Disk. Appropriate plug-ins will be included in future releases of the Gold Disk. The Novadigm Radia server may also push plug-ins to desktops.

3.13.2 Netscape Communicator 4.76

Netscape is included on the NMCI Gold Disk. It is provided as a service for compatibility with existing systems and is not supported by NMCI. All new applications should be developed to support the NMCI default browser, Internet Explorer (version 5.0 or later).

3.13.3 Browser Security

NMCI implements the DoD Mobile Code policy. The DoD Mobile Code Policy defines the categories of mobile code and provides criteria for use within DoD. The policy can be found at the following link: http://iase.disa.mil/policy.html

3.14 EMULATION

3.14.1 Terminal Services

From a developer's perspective, the best standard to follow is Microsoft's guidelines for how to design and construct applications to best run in a "multi-user environment" such as an environment with terminal servers. Microsoft guidelines: Optimizing Applications for Windows 2000 Terminal Services and Windows NT Server 4.0, Terminal Server Edition are available at the flowing URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/win2kts/maintain/optimize/tsappdev.asp.

3.14.2 Products Supported

Reflection is the terminal emulator that is included on the Gold Disk and is a standard application included on every NMCI desktop. Reflection supports IBM, HP, UNIX, Open VMS, and X Suite environments.

3.15 INFORMATION STRIKE FORCE TOOLS REGISTRATION

Developers of desktop applications must register with the current authoritative source for NMCI applications, the ISF Tools Database, which is available by following the transition link at http://www.nmci-isf.com/transition.htm or directly at https://usplswebh0ab.plano.webhost.eds.net/isftool/Login.jsp.

3.15.1 ISF Tools Database Description

The ISF Tools Database is the current authoritative database for NMCI. Application developers/owners must obtain an ISF Tools database account, submit a CDA RFS to ensure their releases are listed and available for certification for NMCI according to Navy enterprise standards and the ISF. The goal is to ensure applications are necessary (rationalized), appropriate and function within the NMCI environment. Once ISF Tools Database access has been granted, a CDA can then do several things with the ISF Tools Database such as, check the status of certification, view application survey data, add additional applications, submit applications, and view reports, all based on the level of access granted by the Echelon POC. For more information,

application developers should download and review the ISF Tools User Manual available on the Login page of the ISF Tools Database or contact the ISF Tools Database POCs. Please see ISF POCs in Appendix C for further assistance.

4.0 SIGN AND DEVELOPMENT – PHASE II

This section focuses on specific requirements the CDA must follow in the development of the release to ensure it is compliant with NMCI standards. It is not the objective of this guide to tell a CDA how to develop a release, but to provide the essential information that will support the certification and testing process covered in Phase III of this guide. It also provides information on the different types of Release Deployments and the information that is required to support each deployment scenario.

4.1 STANDARDS/PROGRAMMING PRACTICES

The NMCI architecture was designed to deliver an integrated family of networks, servers, and workstations configured to support the DON vision for seamless data connection. Therefore, the applications that reside on NMCI must be developed to comply with this architecture and standards.

4.1.1 Microsoft Development Standards

Microsoft Windows 2000 application specification will be used in the development of releases that will be hosted on the NMCI. These specifications will aid the developer in leveraging the new technologies in Windows 2000 to make releases more manageable, more reliable, and reduce development costs.

Development Standards have two versions, the desktop specifications and the server specifications. This document details the requirements for desktop applications. The application must be compliant with the Windows 2000 installer service to ensure the application can be cleanly installed/uninstalled, self repaired, and rolled back on demand. Similar specification for building server applications, are available at the following links: Desktop Spec: (Click here) Server Spec: (Click here)

4.1.2 Programming Guidelines

Microsoft provides specific tuning and optimization guidelines. Adhering to these standards ensures that applications run efficiently within NMCI. These guidelines are as follows:

- Support Customization Through User Profiles
- No Memory Leaks
- Do Not Replace System Files
- Do Not Assume Computer Name or IP Address Equates to Single User
- DCOM Support
- Consider the Peripheral Hardware Environment
- Do Not Assume Persistence of Files in Temp

- Disallowing Multiple Instances of Some Applications
- Do Not Assume the Windows Shell
- Do Not Modify or replace the MSGINA.dll
- Negotiate Client/Server Connections Inside the System and Network
- Multilingual and International Usage Scenarios

4.2 PROGRAMMING STANDARDS FOR A TERMINAL SERVER PLATFORM

For applications to work well in a multi-user environment, certain programming standards must be used. Terminal servers host applications for multiple end-users, but the application must be written so that user-specific information is not tied directly to a machine. For example, applications cannot use the TCP/IP address to uniquely identify a user because many users on a terminal server share the same address. Microsoft provides guidance on the following categories:

- Building a Terminal-Services-Aware Application
- Application Setup in a Terminal Services Environment
- Storing User-Specific Information
- Kernel Object Name Spaces
- IP Addresses and Computer Names
- Client/Server Applications
- Graphic Effects
- Peripheral Hardware
- Background Tasks
- Thread Usage

4.3 USER INTERFACE SPECIFICATIONS

CDAs must consider user interfaces to applications to ensure they meet current and DoD policy, procedures, and standards (DII-COE, C4ISR-AF, DITSCAP, Section 508).

4.4 GROUP POLICY OBJECTS (GPO)

The DON provides a layer of computer defense and control at the desktop by restricting access to the root and system directories (also known as NMCI Boundary 4 security). In other words, the desktop will be “locked down.” The GPO settings and policies will be set by the Navy and implemented by the ISF. In addition, the ISF ensures contract Service Level Agreements (SLA) for the desktop by restricting certain user operations and desktop actions.

The ISF Directory Services Team (DST) administers the desktop and application authentication standards. CDAs need to contact this team when creating or modifying applications for all GPO related issues. CDAs can call the ISF Help Desk.

Please consider the following guidelines when adhering to the GPO:

- Developers are unable to update their Group Policy settings, either locally on their desktop, or non-locally at the AD level.
- Developers must modify releases to comply with GPO policies and Lockdown.
- Developers must go through re-certification processes if their releases fail certification testing (GPO testing).
- Developers need to produce test plans/scripts that include the steps, data, and logical conditions necessary to trigger required authentication processes (Lightweight Directory Access Protocol (LDAP), AD, file sharing, file writes, etc.) to ensure Group Policy, Lockdown, and Security areas are thoroughly examined during Certification in the ISF AIT lab and ISF DST.
- Releases may be permitted to run as a higher credentialed user. This allows the release to run at a user ID level that has the required GPO/Security levels necessary, not as an individual user. Developers are required to program the command set (i.e., run as > userID) and incorporate this in the production environment (script, .bat file, etc.).

The DST provides direction on the necessary code required to accomplish this.

4.5 APPLICATION INTEGRATION TESTING (AIT) GUIDELINES FOR CDAS

4.5.1 AIT Guidelines Overview

The AIT Lab has developed a set of guidelines for CDAs to follow when designing applications. The guidelines are based from the AIT's experience in dealing with GOTS applications in the NMCI Environment. The guidelines are intended to improve the standardization of GOTS applications, which will increase an application's compatibility with the NMCI environment and facilitate enterprise packaging. Standardization will reduce certification processing and troubleshooting time. The guidelines are organized into three categories: Do's, Don'ts, and Recommendations.

4.5.2 Do's:

The AIT lab requests developers adhere to the following points: Adherence to these points will significantly reduce packaging and certification turnaround times.

- Applications are to be installed in the C:\Program Files\Application Name
- Where Application Name is the name of the program.

- Example: “United States Navy Aircraft Maintenance Program” could be shortened to USN AMP. The program will be installed to C:\Program Files\USN AMP. Support files can be installed to other locations, but the main application must be installed in the Program Files folder.
- For Temporary Files, they are to reside in the C:\Program Files\Application Name\Temp folder. The C:\Temp folder, though traditionally a common location to store temp files is not supported in the NMCI environment due to the enterprise software distribution system in use on NMCI. Temporary files must reside in a location in which users have NTFS write or modify permissions. This temp folder within the application’s folder will allow ISF personnel to quickly identify temporary files when troubleshooting.
  Example: “C:\Program Files\USN AMP\Temp”
- For Configuration Files (IE: ini, cfg, sys, etc.), they are to reside in one of two locations depending on the file protection/permission needs.
  - For those files that must or may be updated, they are to be stored in the C:\Program Files\Application Name\Config folder.
  - For those files that require a secured folder to prevent users (and applications) from modifying (note that this is for files which will never need to be modified), the folder is C:\WINNT\System32\CDA\Application Name.
- With the files located in one of these two locations, this will allow ISF personnel to quickly process applications for packaging and certification. The unsecured folder (C:\Program Files…) allows applications to update the files during run-time. By the same token, users will be able to modify these files as well. The secured folder (C:\WINNT\System32…) will prevent users from making any changes to the files; however, applications that run as the user will not be able to make changes either.
  - Example: “C:\Program Files\USN AMP\config.cfg” (modifiable at runtime)
  - “C:\WINNT\System32\CDA\USN AMP\config.cfg” (not modifiable at runtime)
- Data Files (including saved data files and databases) can be stored at two locations: the Local Machine or on a shared folder in the network.
  - For Local Machines:
    - Single User – These are files that are stored and used only by one specific user. These files are to be stored in the “My Documents” folder, previously referenced in this document.
      Example: “C:\Documents and Settings\username\My Documents\USN AMP\Data”
    - Multiple Users – These files can be used by more than one person and usually serve as a common source of data. The locations for these files will be the “C:\Program Files*Application Name*\Data” folder. This allows for ISF personnel to know where the application data files are stored and take proper measures to prevent those files from being updated or overwritten by the

enterprise packaging system.
Example: “C:\Program Files\USN AMP\Data”

- For Shared Folders:
  - Any shared path may be used as so long as the UNC discussed in this document is adhered to.
    Example: “\\SPAWAR\SPOT\CMDSHARE\USN AMP\DATA”

- Application Shortcuts are to be installed to the “C:\Documents and Settings\All Users\Start Menu\Programs\Application Name” folder. This will ensure the shortcuts are created in the Start Menu for all users. This will standardize the location of shortcuts. A side note, the icon (.ico file) of the shortcuts can be of anything ‘non-offensive’, but should not be the default windows icon used when a file cannot be found. If an install package that installs shortcuts is used, care should be taken to ensure only the “All Users” Start Menu shortcut is used. Example: Shortcut path: “C:\Documents and Settings\All Users\Start Menu\Programs\USN AMP\USN AMP.lnk”
- Provide test data with test plan for the application if data files (such as databases) are used. This allows for ISF personnel to conduct tests and be made aware of how the program should function correctly. Based on known test data inputs to the application, know outputs should be generated to ensure the application functions properly.
- For Microsoft Windows Installer (MSI) based applications (applications that use the Microsoft Windows Installer and have files ending with MSI file extension), the MSI package will need to be verified by a test program such as ORCA. The MSI must pass all tests. Invalid MSI based applications will not be packaged correctly by the enterprise packaging system.
- Applications that require the use of a login to run the program will need to have a test login account and a password provided. If no such account information is provided, the AIT Lab will reject applications, as the certification test cannot be completely performed.
- Provide the License and/or Registration keys if the application requires their use. Without the information for those keys, the AIT Lab will reject the application, as the certification test cannot be completely performed.
- Each Application requires a completely filled out RFS form See instructions for this form found at the ISF Tools Database Users Guide on the ISF Tools Log in page.
  - Also the POC is to be listed with the information of someone highly familiar with all aspects of the application.
- Provide a copy of the application’s manual or documentation which will provide information to ISF personnel of how:
  - To install the application.
  - To test the application.

- To operate the program.

- Provide an abstract (overview) of what the application is and does.
- Provide information (release notes) on known or acceptable errors and bugs. Any undocumented error that ISF personnel cannot solve will cause the application to be rejected.
- The applications are to be shipped on 3.5" floppy diskettes or CDs.

4.5.3 Don'ts

This section lists items, which will cause applications to be rejected by the AIT Lab or require substantially increase processing and turnaround time for application certification. The AIT Lab strongly recommends following these items to avoid immediate rejections and shorten the time for certification.

- Do not use desktop shortcuts (shortcuts that are on a user's desktop screen). Desktop shortcuts created from applications are to be kept to a minimum in the NMCI environment. Users are allowed to create shortcuts by themselves.
- Do not compress or zip the pre-installed application. The application would be installed from the diskette(s) or CD(s) without the need to uncompress or unzip. The reason for this is that machines used to package the application for enterprise deployment do not have the capability to uncompress or unzip.
- Do not use the term "Beta" for versioning. An application that contains "Beta" in its version will automatically be rejected, as this application will be assumed to be a pre-production version.
- Example: Use the numeric format for versioning (i.e.,: 2.00.2), instead by words (i.e.: 2.00 Beta).
- The use of modems is not allowed. Do not include any functionality that requires use of a modem.
- Do not support "Uninstall" or "Rollback" in the installation file's executable. Uninstall and Rollback are handled by the NMCI enterprise application management system.
- Do not duplicate any Gold Disk applications or their functionality within the release. http://www.nmci-isf.com/Gold_disk_contents_11.doc

4.5.4 Recommendations:

The AIT Lab provides the items listed below as good tips to allow for quick certification and ease of troubleshooting or updating.

- Use good design programming standards and practices.
- Provide as much clear information as possible about the application. The more information provided, the easier it will be to certify the application.

- Application Configuration files should be in text format. Text based configuration files allow for quick turnarounds in reconfiguring and prevent the need for a complete repackaging of the application for enterprise deployment. Example: An application designed for use at NAS Pax River is requested for use at NAS Lemoore, and is used to be configured on a network. If the application uses text based configuration file, the AIT Lab can make the changes needed to the file within the NAS Pax River package without the need to repackage and test the application. Should the application have the files hard coded/embedded in the application or encrypted, then the program must be completely repackaged and certified.
    - The nature and importance of the application will determine how the configuration files are to be utilized by the developer.
- Keep the size of the application small on the local machines. If the application is large, (the determination of what exactly is considered as 'small' and 'large' is left to the developer's good judgment) please utilize these two possible solutions with the server method most preferred:
    - Use servers to support the large programs or files. As an example a local machine (front end) will have a small program to allow a user to utilize the large database (back end) on a server.
    - Use of CDs is allowed. CDs can be used either in a CD library (where possible) or on the local machines (least preferred).
- Review the latest GPO revisions. The information for GPOs can be obtained from contacting the Eagle Team Facilitator POC for GPOs.
- Schedule and coordinate the testing of the release with AIT personnel to allow CDA participation in the Packaging and Certification Process.

4.6 NMCI INTERFACES

Interfaces to network infrastructure components are commonly identified by reading component specifications. Proper interfacing with enterprise infrastructures is required to ensure that the infrastructures continue to operate according to their original design and capacity.

This section identifies infrastructure interfaces, Application Program Interfaces (APIs), and specifications for the various types of applications that will share the NMCI/IT-21 network environment. Developer responsibilities and common approaches to these interfaces will be enumerated in an effort to protect, respect, and maximize the investment in the common enterprise network infrastructure. The goal for a developer should be to develop NMCI/IT-21/ MCTN applications that will work securely and harmoniously with common network resources. Both NMCI and TFW participate in this object model via AD.

An excellent resource for information pertaining to Win32 API, and Microsoft's Active Directory Service Interface (ADSI) model is available at http://www.microsoft.com/windows/reskits/webresources.

4.6.1 Windows 2000 Desktop Application Interface Specification

Microsoft provides the Windows 2000 standard desktop specification at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli.asp. This section describes the standard Windows 2000 APIs used in NMCI workstations and discusses NMCI's use of Novadigm Radia (a software distribution system) and AD technologies that manage resource availability of both software and hardware, based on workstation or NMCI end user accounts.

Desktop applications developed for NMCI Windows 2000 environment must undergo an ISF certification process, enumerated in Phase III, prior to deployment within the NMCI environment. The NMCI environment, monitored by the ISF, will protect connected user workstations, data, and application servers if and only if developers or users interfacing with the network need guidance. Both applications and users will be controlled as objects and removed from participation in NMCI should they violate policy or specifications.

4.6.2 Microsoft Windows 2000 Server Interface Specification

Microsoft provides the Windows 2000 standard server specification at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2ksrv/html/w2kserve.asp. This specification provides resources to attain Windows 2000 certification (including checklists) and receive the Microsoft Windows 2000 logo. Meeting the Microsoft Windows 2000 logo specification will produce a release that is NMCI compliant. However, a developer may encounter situations in which applications must be developed which do not meet all Microsoft Windows 2000 logo specifications. In cases where the GPOs, directory permissions, AD, firewall policy, and other settings cannot be met, the developer should contact the ISF Help Desk for guidance.

4.7 SIMPLE (STANDALONE) APPLICATION

A simple application, for the purpose of this section, may be defined as a standalone application that requires installation on an NMCI workstation and has a small number of primary functions that do not require backend connectivity to any network. An example: Windows "calculator" application on most Windows computers.

4.8 COMPLEX (CLIENT/SERVER/ NETWORK SENSITIVE) AND MOBILE CODE

Applications that require network connectivity for standard operation may, for the purposes of this guide, be defined as "network sensitive." These applications must use TCP/IP in a bandwidth efficient manner to ensure the ISF can maintain network SLAs.

4.8.1 Mobile Code

Mobile Code is a powerful software tool that enhances cross-platform capabilities, sharing resources, and web-based solutions. Its use is widespread and increasing in both commercial and government applications. In DoD mobile code is employed in systems supporting functional areas ranging from acquisition to intelligence to transportation. Mobile Code is not restricted from use within NMCI but when used it must be fully compliant with established DoD standards. Mobile code, unfortunately, has the potential to severely degrade DoD operations if improperly used or controlled. More detailed information on Mobile Code can be obtained from the following web site at: http://iase.disa.mil/policy.html.

4.9 BOUNDARY/NETWORK INTERFACE SPECIFICATIONS

The type and strength of each security component is dependent upon the information protection requirements for a particular system. Boundary 1 reflects the Navy Marine Corps Enclave Protection Policy. Boundaries 2 and 3 security mechanisms are flexible enough to meet the security requirements of various scenarios. Boundary configurations are tailored to provide the level of protection necessary to protect the integrity of NMCI and its users. NMCI also provides a wide-area IP backbone using Defense Information Systems Agency (DISA) Wide Area Network (WAN) services with Very High Speed Backbone Network Service (VBNS+) transport services. The Transport Boundary (TB) offers a secure encrypted intranet path between bases while imposing minimal restrictions on inter-base communications. Specific technical information on boundary requirements is available by contacting ISF IA personnel or the NMCI DAA.

Each system or application uses protocols to communicate between clients and servers. Many protocols and ports are associated with security vulnerabilities, and boundary policy reflects this. If an external application is compliant with Boundary 1 firewall policy, then users within NMCI may access the application through the B1 boundary. To know if an application or system is compliant, its protocols, ports, and directions of activity must first be identified and characterized for assessment with respect to those of NMCI.

If an external system requires interaction not allowed by Navy/Marine Corps firewall policy, there are technical methods to obtain access through the boundary. The Navy/Marine Corps may choose to make a modification to the baseline firewall policy to permit access to a system. Access may be possible through a Virtual Private Network (VPN) path. A risk assessment must be prepared to determine whether a modification to firewall policy or use of a VPN is acceptable. The NMCI DAA and local DAA will use C&A documents to assess risks and make firewall policy modifications. A risk assessment does not need to be a one-at-a-time process: several applications can be considered simultaneously, if they run on shared servers and use the same ports/protocols.

4.9.1 Transport Boundary (TB)

The TB is a suite of network security components configured to provide WAN network security.

4.9.2 Boundary 1 (B1)

The B1 resides at the NOC and is designed to protect access to NMCI from the Non-Secure Internet Protocol Router Network (NIPRNET) and Secure Internet Protocol Router Network (SIPRNET). This boundary protects NMCI users and services located in external networks (i.e., IT-21, MCTN, DISN). The specifications for B1 can be found at the following web site: https://www.infosec.navy.mil.

4.9.3 Boundary 2 (B2)

The B2 resides at the site and is designed to interface NMCI with the site legacy network. The B2 allows application reach-back into the legacy network. The B2 is an evolving security component that will no longer be employed once all Navy and Marine Corps networks are migrated to NMCI. The specifications to the B2 can be obtained from the NMCI DAA (NETWARCOM).

4.9.4 Boundary 3 (B3)

The B3 is provided for use by COI operating within the NMCI network.

4.9.5 Boundary 4 (B4)

The B4 is composed of those measures taken to ensure secure operations and communications at the workstation or desktop level. This is accomplished through four primary methods: GPO Settings, Virus Protection, Intrusion Detection, and Compliance Management.

4.10 NETWORK RELATED API'S OTHER THAN STANDARD WIN2K API'S

Microsoft ADSI may prove useful in realizing the enterprise benefits of AD and can be found here: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active_directory_service_interfaces_adsi.asp).

4.11 NMCI LOCKDOWN POLICY

NMCI lockdown policies disseminated through the AD, and enforced via GPOs, are highly restrictive settings that differ from the recommended Windows 2000 GPOs. Essentially, the application may write to its own area of a workstation disk with administrator privileges during install but then must refrain from writing to restricted portions of the registry or other non-authorized areas of the disk at runtime.

4.12 SOFTWARE INSTALLATION

For pushed or remote installations, the installation script will be run as administrator, but the same lockdown policy applies at runtime. Applications deployed to NMCI clients should be placed in a folder under the directory C:\PROGRAM FILES.

4.13 SCREEN SAVER

NMCI desktops are set with the NMCI ISF screen saver. The screen saver will activate after 15 minutes of inactivity and the user will prompted for a password to log back into the active desktop. The desktop user cannot change this.

4.14 TERMINAL SERVICE

From a "terminal service" perspective, "NMCI Thin Client" architecture supports Windows 32-bit applications. The Citrix components (Nfuse, etc.) can interoperate with the NMCI portal. This makes it possible to launch PC-based applications from the portal, display across the intranet, and appear to run locally while running remotely.

4.15 TESTING CONSIDERATIONS

Applications must successfully complete the Developer Test and Evaluation (DT&E), including the creation of test scripts and test cases. It must be verified that the application will work on an NMCI-certified workstation. Developers must describe the types of tests done in the NMCI Certification process (e.g., will the application print?; will MS Office applications continue to operate?); any consideration for prototype/pilot testing; the steps, data, and logical conditions necessary to trigger programmed authentication processes (LDAP, AD, file sharing, file writes, etc.) to ensure Group Policy, Lockdown, and Security areas are thoroughly examined by the Certification and DST. Developers must ensure logon IDs have the same access rights as end-users, not developers. For detailed instruction on the DT&E contact the ISF AIT.

5.0 RELEASE DEPLOYMENT – PHASE III

Integration of a release within NMCI requires application developers to complete several review and test processes. This section defines the processes that a release must undergo for certification in the NMCI. The major steps in the process and basic considerations are described in this section but for updated instructions on specific areas be sure to check with the ISF Tools Database at: https://usplswebh0ab.plano.webhost.eds.net/isftool/Login.jsp.

5.1 APPROVAL TO DEPLOY

Before a CDA can begin the deployment cycle, the CDA must receive authorization to deploy the release in NMCI. The request to deploy process was introduced in chapter 2 in this guide.

- Completion and submission of RTD
- Approval to deploy from NETWARCOM
- Priority established by NRPM
- Release scheduled by NRSM

5.2 NMCI APPLICATION RELEASE DEPLOYMENT PROCESS

The NMCI Application Release Deployment Process depicted in *Figures 5-1 and 5-2* below, covers the testing, certification, and deployment processes that releases must undergo to ensure the security and integrity of the NMCI network. The process ensures that all releases are compliant with established standards, directs actions to be taken when compliance is not achieved, and covers steps involved in the deployment of the release.

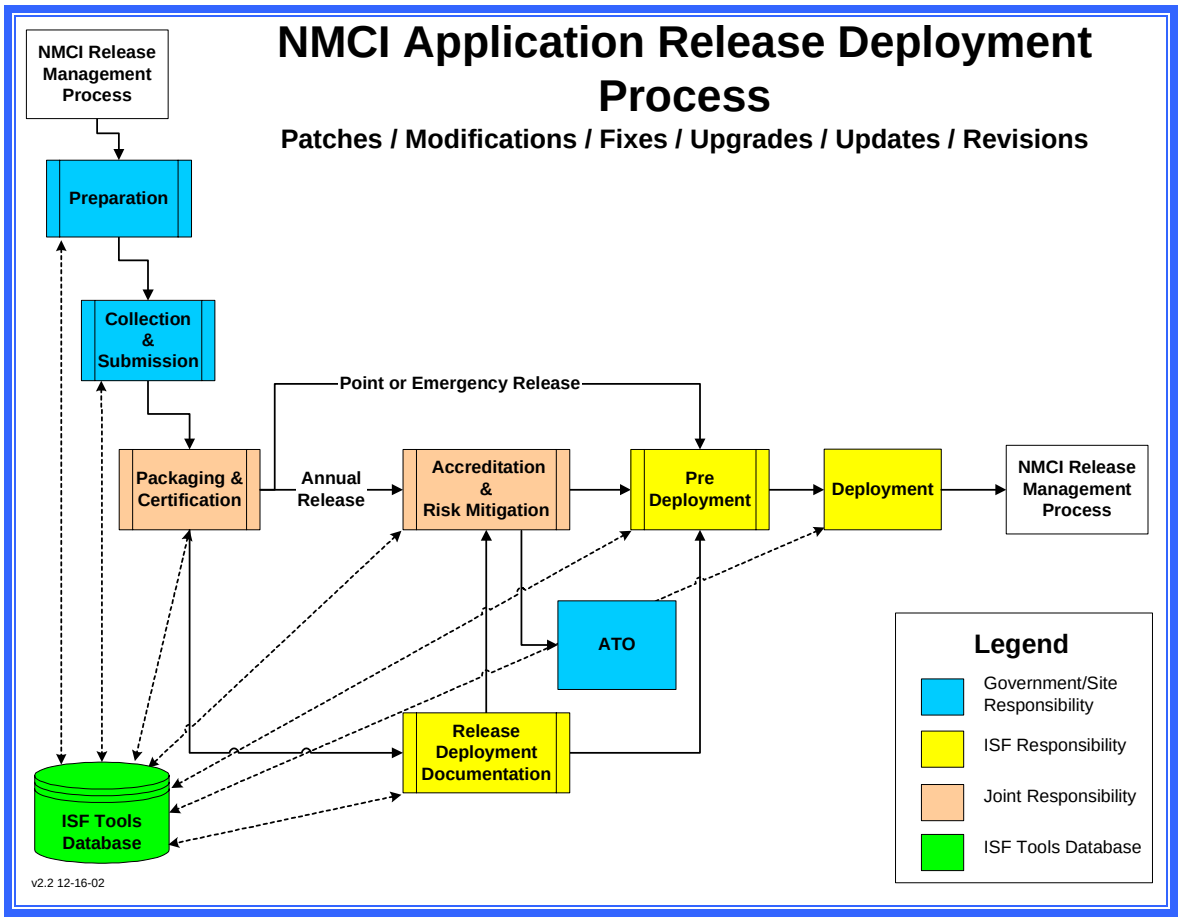


Figure 5-1 NMCI Application Release Deployment Process

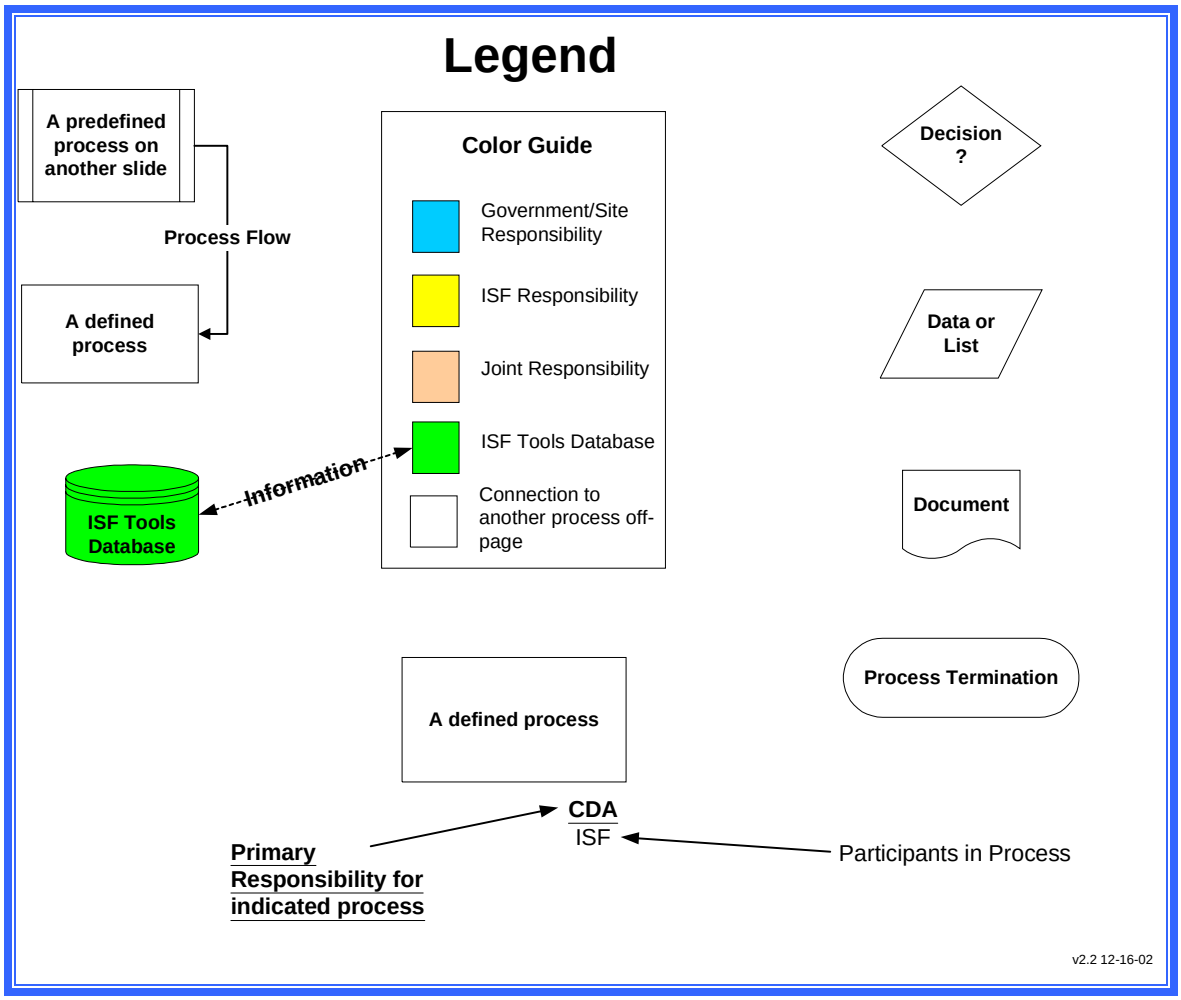


Figure 5-2 NMCI Application Release Deployment Process Legend

5.3 TIMELINE FOR NMCI APPLICATION RELEASE DEPLOYMENT PROCESS

5.3.1 Release Timing

In order to maintain control and discipline in the NMCI environment, a formal submission and deployment process will be followed. *Figure 5-3* depicts the notional timeline for submitting and processing a release. Again, this time is notional and meant as a guideline. A release may transition this timeline in less time than depicted. However, this timeline is designed to process any size release in no more than the 90 days indicated. The Application Release Deployment Process for any release follows the pattern from left to right.

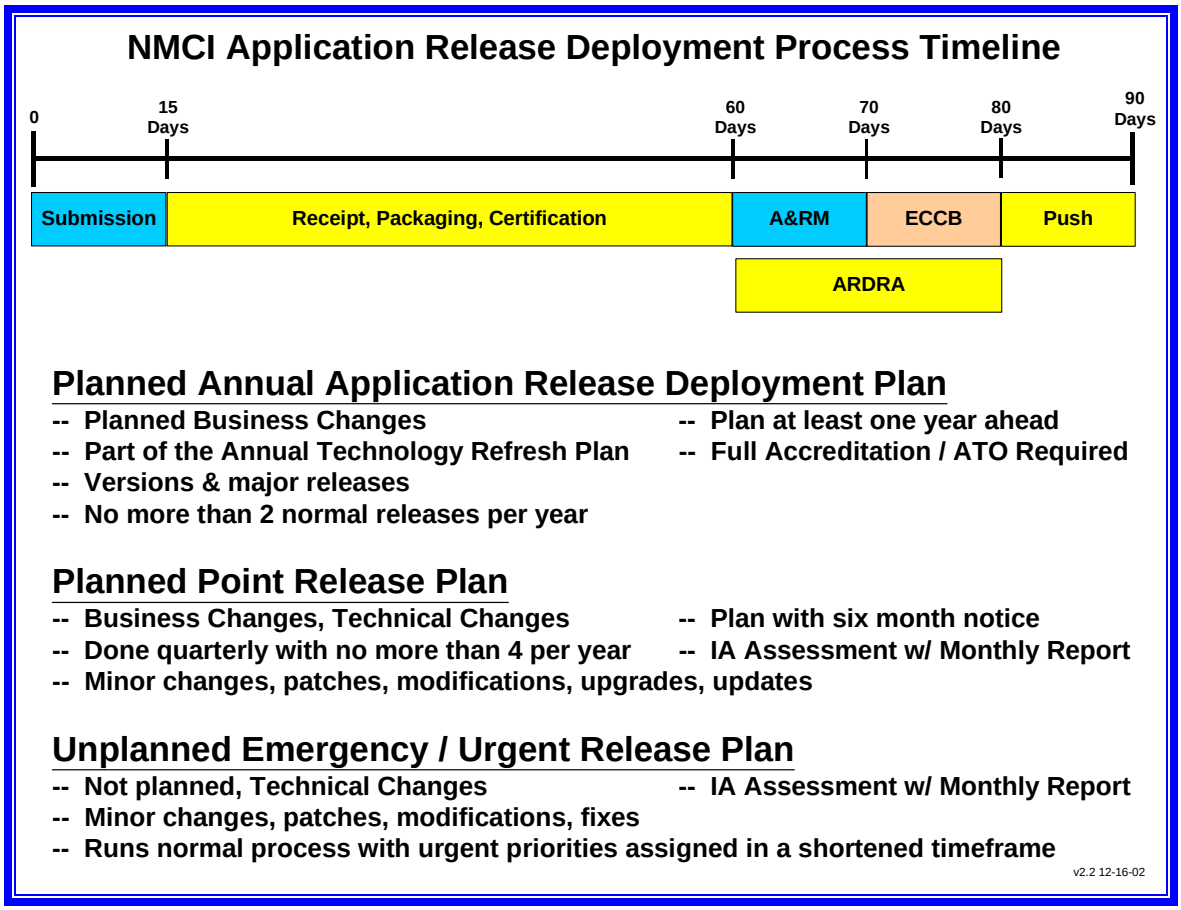


Figure 5-3 Timeline for NMCI Application Release Deployment Process

5.3.1.1 Submission (Days 1 - 15)

The typical 15-day release submission window is utilized for all releases into NMCI. To avoid overwhelming the system, CDAs will be assigned a specific submission window to submit their releases for processing. Except for emergency releases, all other submissions must be within the appropriately assigned submission window. Missing the assigned submission window will require the CDA to hold the release until the next appropriate submission window. The CDA will have the release developed, complete and ready for submission prior to the beginning of the submission window.

5.3.1.2 Receipt, Packaging, Certification (Days 15 - 60)

The next segment of the timeline in the Release Deployment Process is the Receipt, Packaging and Certification Processes. The ISF will process the release in the AIT lab and Network Operations Center (NOC) in San Diego. The application is received, packaged, client tested, connectivity tested (if needed), certified, with status maintained in the ISF Tools Database. The CDA is required to participate in this testing. Though this segment is notionally depicted as 45 days, it may be much less depending on various factors.

5.3.1.3 Accreditation and Risk Mitigation (A&RM) (Days 60 - 70)

A&RM is required for annual releases and those releases that have an impact on the IA posture of an application. The supporting documentation for the A&RM process actually starts the moment a release in conceived. This ten-day period includes the finalizing and submission of the Accreditation and Risk Mitigation (DITSCAP and NCAP) package.

5.3.1.4 Application Release Deployment Readiness Activity (ARDRA) (Days 60 - 80)

ARDRA is a parallel process that actually starts once the packaging, certification, and testing in the AIT and San Diego NOC labs is complete. These 20 days are used to address any testing needed to ensure a successful deployment at the sites/bases involved. ARDRA is conducted on-site and is not a mandatory step, but is used when a specific deployment concern needs addressing at the site. The decision to pre-test the release for deployment rests jointly with the specific ISF SM and the CDA.

5.3.1.5 Enterprise Change Control Board (ECCB) (Days 70 - 80)

The final release solution and IA impacts for a release are submitted for review and approval by the ECCB. A formal ECCB output and approval is required for all annual releases and those point/emergency releases that have an IA impact.
Note: This step has not been determined nor implemented yet and will be deferred until the concept is fully developed within the NRMP.

5.3.1.6 Release Push / Deployment to the Desktop (Days 80 - 90)

Once the release has completed all testing and received all approvals, it is pushed or locally loaded to the desktop. ISF SMs and CDAs play an important role in these steps.

5.4 PREPARATION

During the Preparation process the CDA begins to develop the detailed RDP that will document release information and data used throughout the development and deployment process. Precertification consists of the CDA obtaining important information that will be used by the ISF later in the Release Deployment Process. The ports and protocols are captured, and the network diagram is developed or updated as necessary. *Figure 5-4* depicts the Precertification process through which the CDA will test the release to determine compliance with Windows 2000, NMCI Boundary, Gold Disk, and GPO standards. The CDA then completes the following tasks:

- Capture Ports, Protocols and Services
- Develop/Update Network Diagrams
- Update RDP to reflect any changes made.

CDAs must consider submission widows for annual and planned point releases and requirements for ECCB approval for all Emergency/Urgent releases prior to proceeding to the Collection and Submission process.

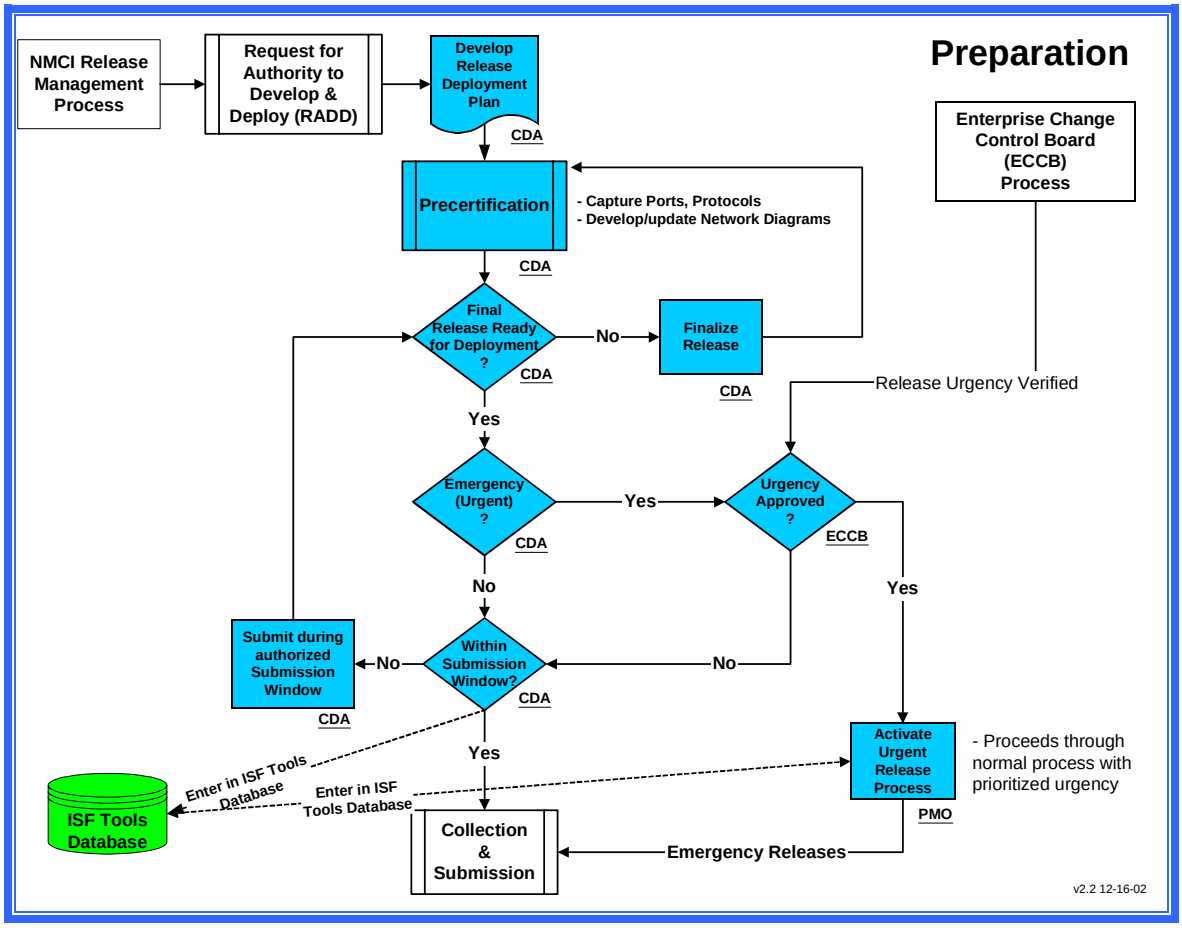


Figure 5-4 Preparation Process

5.4.1 Precertification Information

The CDA conducts a Precertification test on the release for NMCI functional compliance. This consists of testing the release to ensure it is Windows 2000, B1 and B2 Boundary, Gold Disk, and GPO compliant. *Figure 5-5* depicts the Precertification process is designed to run the release in an NMCI operating environment to test compliance. If an error is detected, the CDA will be required to fix the problem before the release can move on to the next process. The information gathered during Precertification will allow ISF to deploy the release quicker and more efficiently.

CLIN 0029 is in the process of being revised to provide the CDA with a fee for service test box to perform release precertification testing. The CDA will have the option of selecting the test box that best supports their need and funding capability. The cost of test boxes will vary

depending on if support personnel are required to support testing. To support this process, the ISF has built a visual basic tool, the AutoCert/Automated Post Local Installation Test (APLIT). This tool automates the testing of a release against the Gold Disk. The three categories specifically tested are the MS Office Suite, Windows applications, and 3rd party software. The tool will report any errors the release has with the Gold Disk.

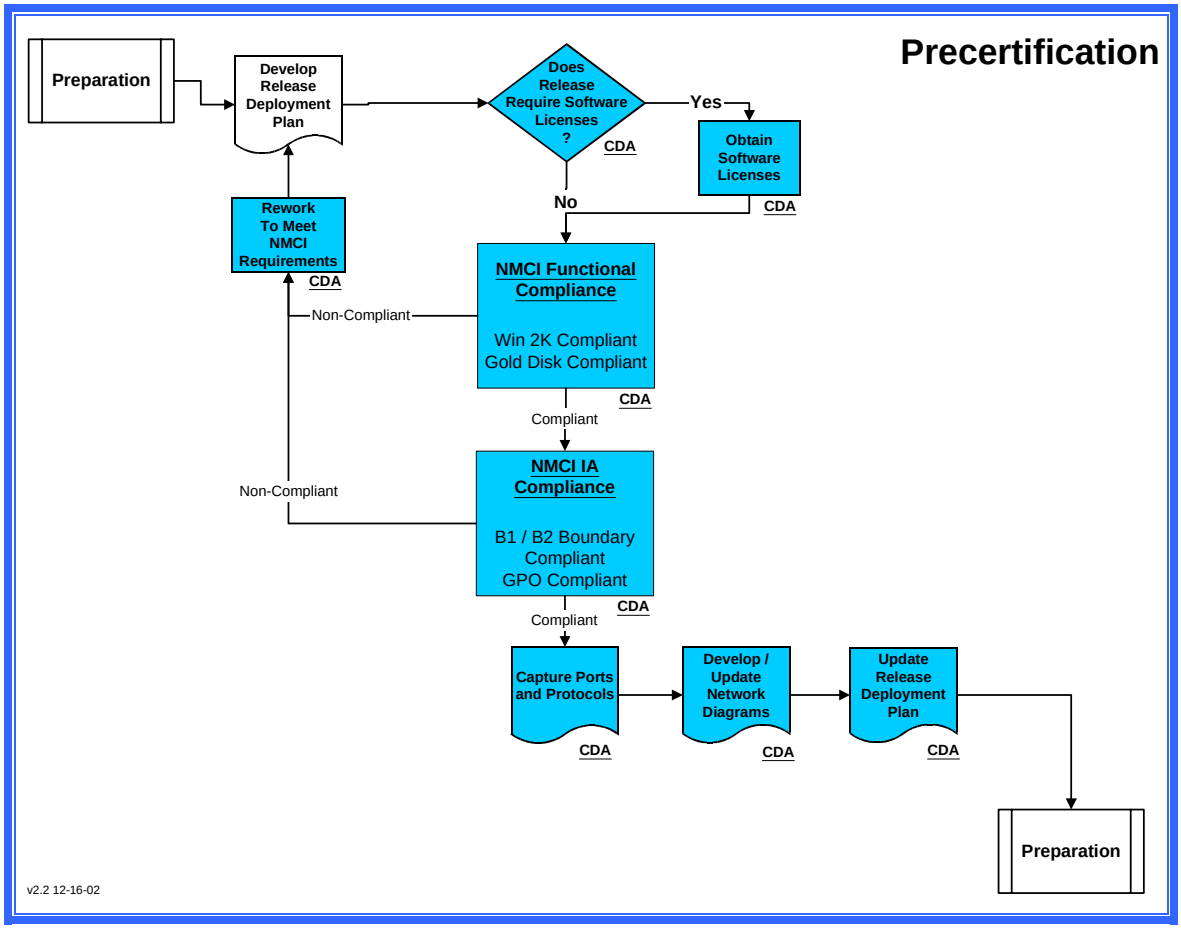


Figure 5-5 Precertification Process

5.5 COLLECTION AND SUBMISSION

Figure 5-6 depicts the Collection and Submission Process. The CDA begins this process by generating a RFS using the ISF Tools Database. Additionally, the CDA updates the RDP with the following required information:

- Copy of the Completed RFS
- Installation instructions
- Licenses and Media
- Detailed test scripts

- Desktop and Server Connectivity Diagram
- Identify affected sites (UTAM) - The CDA will identify the sites, servers and users that will receive the release. The ISF will use this information to ensure that the release is deployed to the proper sites, servers, and users
- Precertification Ports and Protocols
- A copy of the Engineering Review Questionnaire (ERQ) (annual release only).
- Release Lifecycle Technical Support Plan
- The CDA must include the IATO/ Authority To Operate (ATO) and DITSCAP documentation if applicable (for an annual release only)

See Appendix I for samples, examples and templates.

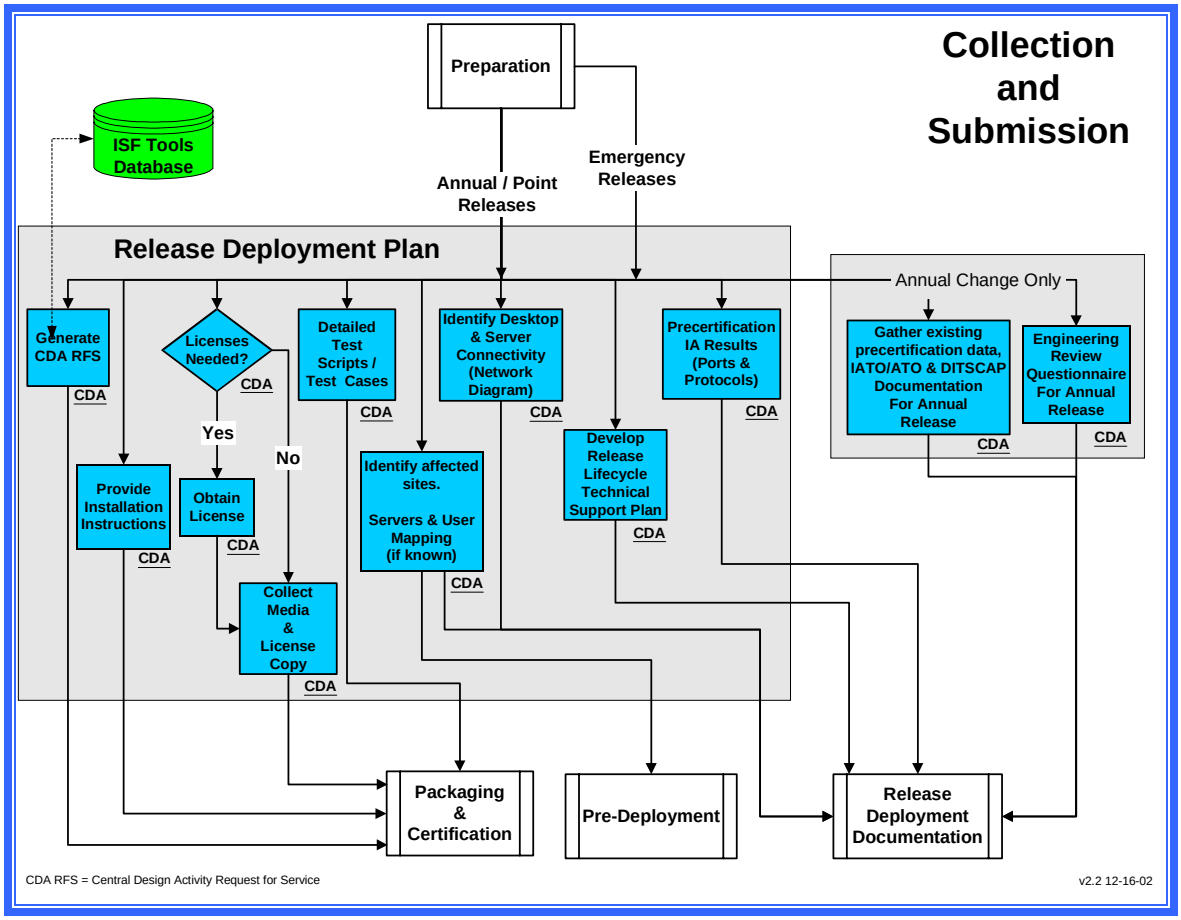


Figure 5-6 Collection and Submission Process

5.5.1 Release Lifecycle Technical Support

The CDA must develop and implement a Lifecycle Technical Support Plan (LTSP) for the release. This technical support plan will provide a detailed roadmap for escalating release

troubleshooting to the appropriate technical support level. This includes directing Help Desk personnel and the trouble ticket system in assisting the users in resolving technical problems by the appropriate release technical support personnel.

The LTSP will be included as part of the Release Deployment Plan. The details of the LTSP are part of the NMCI Release Management Plan and the instructions for this plan are not included in this document.

5.6 PACKAGING AND CERTIFICATION

The Government and the ISF share joint responsibility in this process, but the ISF conducts the majority of the work. A CLIN 0029 revision is being developed for requesting testing services from the ISF. Pricing for CLIN 0029 was not available at the time this guide was published. The ISF AIT laboratory in San Diego has the responsibility for auditing, testing, packaging and final certification of the release to operate within NMCI. *Figure 5-7* below depicts the Packaging and Certification process.

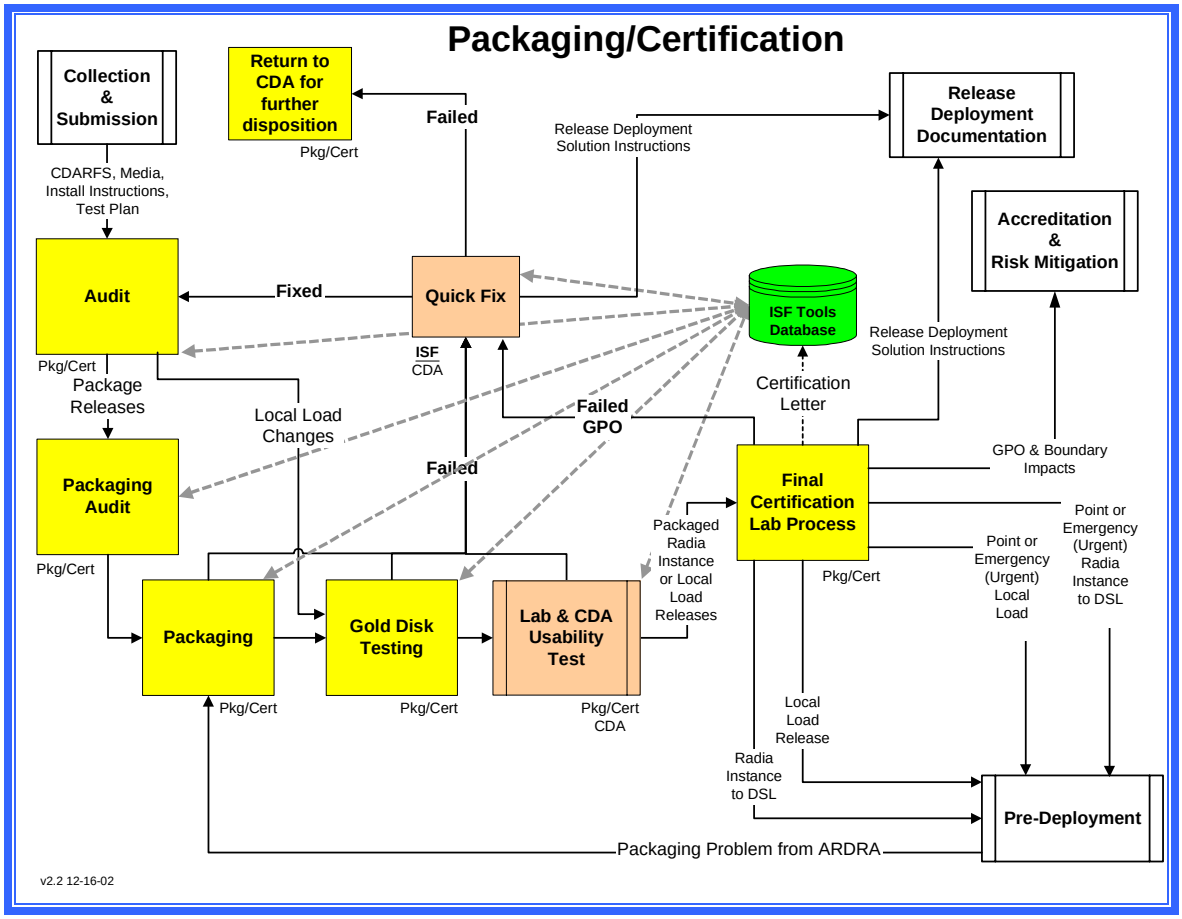


Figure 5-7 Packaging and Certification

5.6.1 Audit

The audit process ensures all required documents are correct and complete along with a clean version of the release. During this phase of Packaging and Certification the ISF is responsible for determining the most effective way to deploy a release. This determination employs several criteria including user count and enterprise impacts.

5.6.2 Required Documents for Audit

The following documentation is required during audit:

- CDA RFS
- ERQ (for annual release only)
- IATO, ATO, and DITSCAP documentation (for annual release only)
- Release Media
- Installation instructions
- Test Scripts (including Precertification results).

5.6.3 Release Distribution

As part of the audit process, ISF (with the CDA) will determine which method of deployment will be used for that particular release. ISF uses an enterprise-wide application deployment system to serve as the standard Enterprise Desktop Manager (EDM) product to support an enhanced level of software distribution and management. All releases that are to be pushed will be distributed through a Radia instance push. No matter what users do to break their individual desktops such as deleting files, installing conflicting software, or changing their desktop configurations, the Novadigm manager will automatically identify the problems or incompatibilities and adjust the desktop just in time ensuring the remote stays up and running.

5.6.3.1 Push

Releases with a high user count and exposure are likely to require an enterprise solution for deployment and maintenance. The ISF has selected an enterprise-wide application deployment system to provide a centrally managed capability to support the Push process.

5.6.3.2 Local Deployment

Releases with a low user count and local impact are more likely to require a local deployment. Local deployment options can include a desktop install and a central server install. Releases that are designated as local deployment will not undergo package processing.

5.6.4 Packaging

All Push releases that successfully complete audit are packaged into an instance using Enterprise wide application deployment system. If the release fails packaging for any reason, it

is sent to Quick Fix for problem resolution in the lab. Quick fixes that cannot be resolved are returned to the CDA for further disposition.

5.6.5 Gold Disk Testing

All releases undergo Gold Disk Testing to ensure there are no interoperability or compliance problems with the Gold Disk. If the release fails the Gold Disk Test it is sent to the Quick Fix for problem resolution. When errors are corrected the release is retested and submitted for Lab & CDA Usability Test.

5.6.6 Lab & CDA Usability Test

The Lab & CDA Usability Test is a sub-process of the Packaging and Certification. *Figure 5-8* depicts the Lab & CDA Usability Test Process. The Usability Test verifies the Precertification IA results provided by the CDA during the Collection and Submission of the release. When annual releases are being tested, it is vital that the CDA be present. In the event of a problem, the CDA, or a representative thereof, can assist in the Quick Fix (paragraph 4.1.9) of the release. Planned point release and emergency/urgent releases are not expected to cause any major problems and therefore may not require the presence of the CDA.

The Lab & CDA Usability Test is conducted in the ISF AIT Lab in San Diego in an isolated NMCI environment. This test will be performed on either a release that has been newly packaged, or a release designated to be locally loaded. The packaged release is pushed to or the local load release is loaded to a test cell in the AIT Lab.

If there are any special configuration changes needed to get the release to install properly, that configuration information is documented in the ISF Tools database and the RDP. The site user/application owner/CDA will assist with any required configuration changes.

The AIT lab personnel will run the network diagnostics using a sniffer (EtherPeek software) to trace the ports, protocols, and services used by the release. The test results will be documented and sent to ISF IA personnel. Each release is also reviewed for compliance with Boundary 1 (B1) and Boundary 2 (B2) firewall policies.

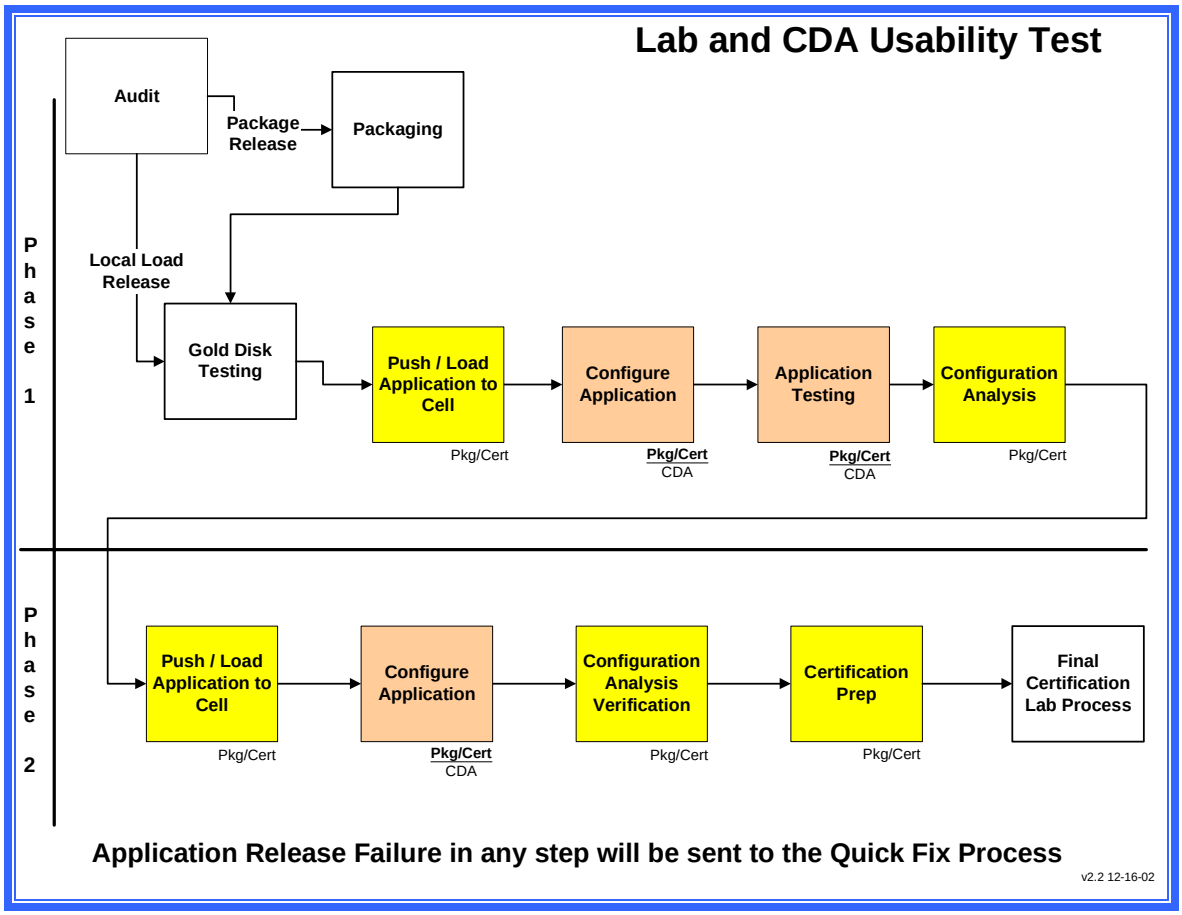


Figure 5-8 Lab and CDA Usability Test

5.6.7 Quick Fix

If a release fails the Packaging, Gold Disk Testing or Lab and Usability Testing, it undergoes the Quick Fix sub-process. The Quick Fix sub-process goal is to identify and apply a rapid, easily applied solution for the release to meet final certification and packaging requirements. The AIT Lab or the release owner/CDA shall work together to identify the applicable solution(s). After the solution is identified and applied, the release is returned to the Packaging and Certification process. The Release Deployment Solution Instructions are updated when the release is fixed and sent by the ISF to be stored as Release Deployment Documentation. These instructions are included in the RDP found in Appendix G.

If a problem cannot be readily resolved at the AIT Lab, the release is returned to the CDA for further action. If the CDA still desires to deploy the release, the problem must be corrected before the release can be resubmitted during the next submission window.

5.6.8 Final Certification Lab Process

Once the release has successfully completed testing a certification letter will be issued and included in the Release Deployment Plan.

At this point, two things will occur. First, the NMCI Certification Letter is created by the AIT lab and entered into the ISF Tools Database. Second, the Release Deployment Solution Instructions are sent to the Release Deployment Documentation. A copy of the Certified Packaged Instance is stored at the Definitive Software Library (DSL). The DSL is a system storage repository of all packaged instances that have been through the final NMCI approval processes. These are instances that are ready for immediate deployment when executed by the ISF.

During the Final Certification Lab Process, Boundary and GPO impact release information is collected and used in the Accreditation & Risk Mitigation Process for the annual releases. Planned point and emergency releases go directly to the Pre-Deployment process.

5.7 RELEASE DEPLOYMENT DOCUMENTATION

Before releases proceed to the AIT Lab for Packaging and Certification, the CDA must prepare Release Deployment Documentation as depicted in *Figure 5-9*. This process consists of the following:

- The identified desktop and server connectivity (Network Diagram)
- The updated Release Deployment Plan
- The IA results (ports, protocols, and services)
- Provide existing accreditation documentation, to include: ATO, IATO, and DITSCAP
- ERQ located at http://www.nmci-isf.com/transition.htm#Engineer

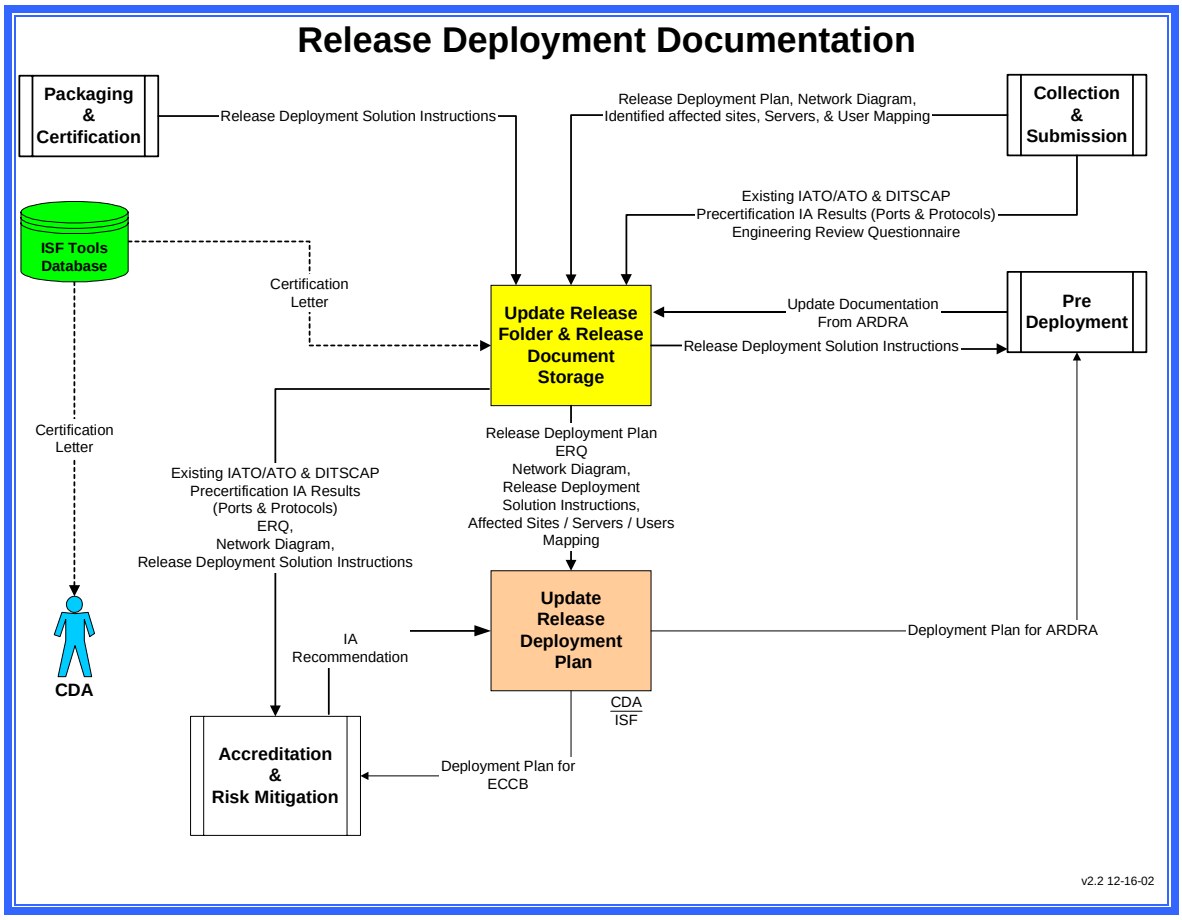


Figure 5-9 Release Deployment Documentation

5.8 ACCREDITATION AND RISK MITIGATION

The Accreditation & Risk Mitigation Process depicted in *Figure 5-10* is a Government responsibility. Only the annual releases go through this process. In this process, the IA impact of the release is reviewed and a full ATO will be issued upon completion of this process. ATOs are sought for annual releases due to the time a CDA has to prepare for the submission of the release.

It is the responsibility of the CDA to obtain an ATO or IATO through the DITSCAP process for each application. In general, an IATO or ATO granted to an entire site or command is not acceptable unless the documentation demonstrates that the application has been tested and approved. The IATO/ATO must be valid for at least six months after the date of submission. An application whose IATO/ATO expires will be removed from the NMCI network until a new IATO/ATO is received. The annual release information is used to obtain full accreditation and an ATO. Annual releases will have sufficient lead-time to obtain the ATO. Once the CDA completes Collection and Submission, the release is now ready for submission with required documentation to ISF for Packaging and Certification.

The NMCI DAA releases Vulnerability Reviews of the release based on the following information:

- Boundary/GPO impacts
- Existing ATO, IATOs and DITSCAP documentation
- Precertification IA results (ports & protocols, network diagram)
- ERQ
- Release Configuration Sheets

The Vulnerability Reviews are included in the Monthly Release Report. Once distributed, the DAA looks at the IA impact of the release. The DAA verifies that the CDA has met the IA requirements. If the DAA discovers any IA impact, the CDA is informed. The CDA must then re-engineer the release to meet NMCI requirements. Once these requirements have been met, the CDA can resubmit the release in the next submission window.

If no IA impact is found in the release information, then it is incorporated into an IA Vulnerability Assessment Package (IVAP). This includes:

- IA recommendations
- GPO impacts
- Type Accreditation B2 Boundary Firewall Policy Impacts
- Navy/Marine Corps Enclave Protection Policy (B1 impacts)
- Certification Letter

The CDA enters the IA recommendations into the Release Deployment Documentation and finalizes the Release Deployment Plan. The GPO impacts undergo the ISF GPO Rules Recommendation sub-process to determine if the GPO needs to be modified.

The other three components undergo NMCI DAA review and approval. The DAA reviews and approves the Boundary policy impacts and the ISF builds the Boundary Rules. The ISF ECCB reviews these Boundary Rules modification recommendations.

The ISF ECCB looks at the Final RDP and any changes to the Boundary or GPO rules. After reviewing this information, the ISF ECCB approves and sends the IA rules documentation for deployment to the Pre-Deployment process.

5.8.1 Actions of the ISF Enterprise Change Control Board (ISF ECCB)

The ISF ECCB is composed of personnel from EDS, the Navy, the Marine Corps, and the PMO. IA and operations personnel from the Navy and Marine Corps will work with the ISF and the PMO to assess the overall risk exposure. Additionally, the necessity of the application in the enterprise is examined. The ISF ECCB reviews all submitted documentation. Releases that meet all ISF ECCB requirements will be approved to continue in the deployment process.

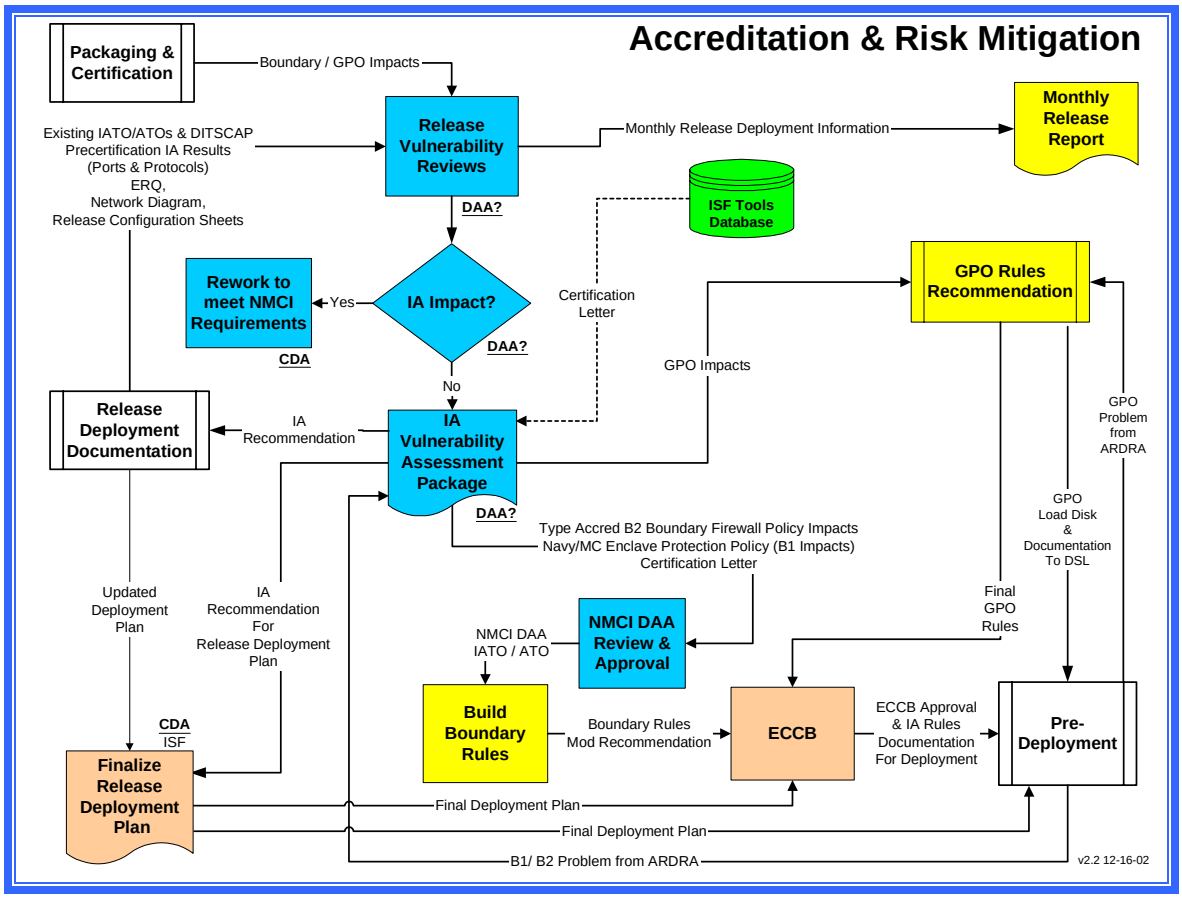


Figure 5-10 Accreditation & Risk Mitigation

5.9 PRE-DEPLOYMENT

The Pre-Deployment process as depicted in *Figure 5-11* is primarily an ISF responsibility. In this process, final preparations are completed before the release is deployed to user seats. There are several milestones before ARDRA, or pre-deployment test can begin. These milestones are:

- Enterprise Boundary 1 is in place at the NOC
- Enterprise Boundary 2 and GPO are deployed
- Final Deployment Plan is completed
- Release Deployment Solution Instructions are ready
- Local Deployment releases are ready
- NOC is ready to “push” releases to seats.

Two things must occur before the NOC can accomplish the push; (1) the Radia Instances must be loaded from the (DSL) to the San Diego NOC, and uploaded to the designated NOC; (2) Base Operations updates the User Profiles in AD using the sites, servers and user mapping information received from the CDA.

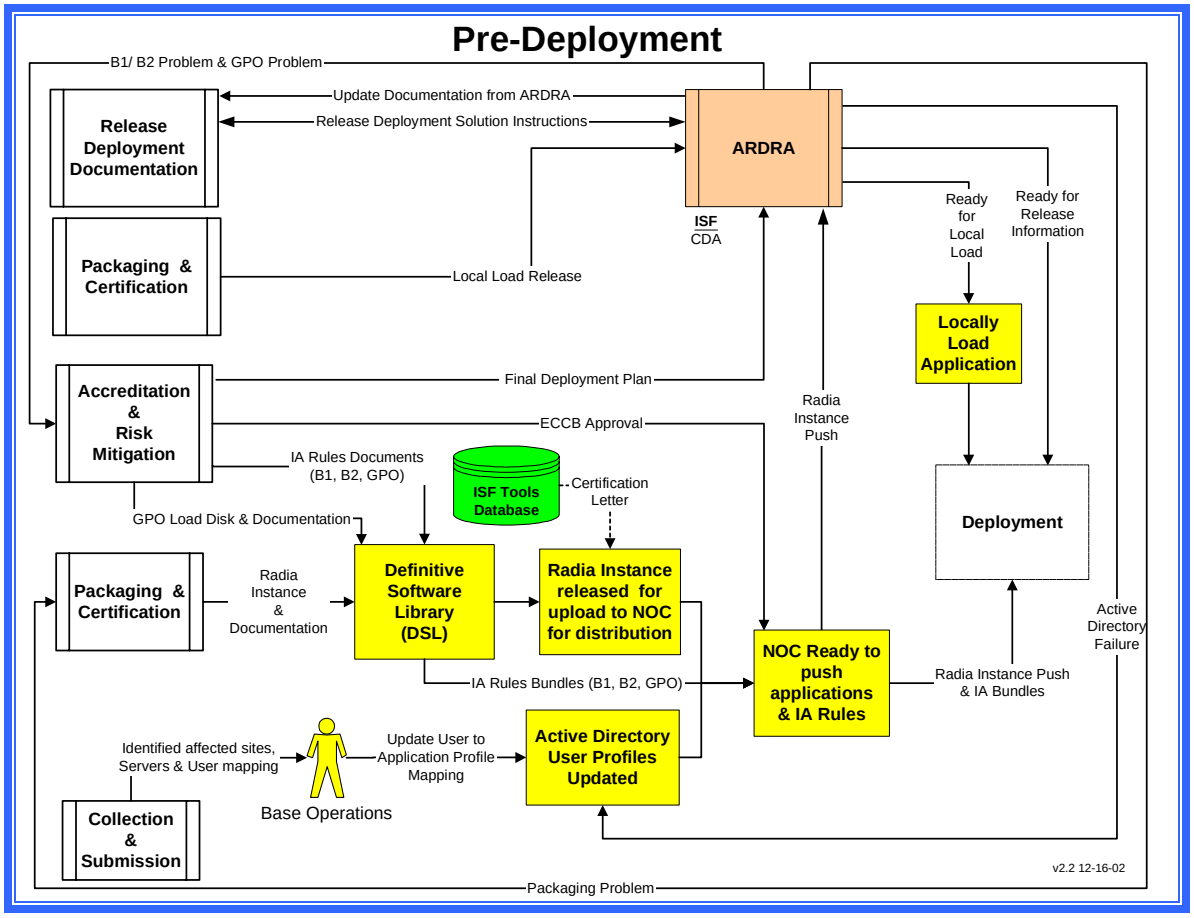


Figure 5-11 Pre-Deployment

5.9.1 Application Release Deployment Readiness Activity (ARDRA)

ARDRA testing as depicted in *Figure 5-12* is the final test a release will undergo. It is not a substitute for Alpha/Beta testing, but is a verification test of final release configuration, NOC connectivity, boundary policies, and documentation prior to deployment. Generally ARDRA is utilized to perform final pre-deployment testing on complex releases. However, ARDRA can be performed on any release. The decision to conduct ARDRA resides with the ISF with input from the CDA. The ISF/CDA may opt for an ARDRA test or deploy the release without conducting one. ARDRA testing is conducted by the ISF Base Operations in the live NMCI environment. The objectives of ARDRA are to:

- Evaluate the performance and IA policies of Certified DSL releases. This can include unclassified/classified COTS and GOTS in a true NMCI production environment.
- Provide on-the-job-training for select NMCI Desktop Deployment and ISF Base Ops personnel on the manual configuration of releases.
- Ensure proper network configuration and operation

- Evaluate migration tools
- Evaluate Radia applications management
- Validate migration implementation plan and test print functions

NOC pushes the release to test seats set up for ARDRA. The ISF Base Operations verifies that the "push" occurred, and that the release installed properly. Any manual configuration changes needed for the proper installation of a release are noted and analyzed. If these configuration changes can be integrated into the Radia Instance, the release may be sent back for repackaging and NMCI Certification.

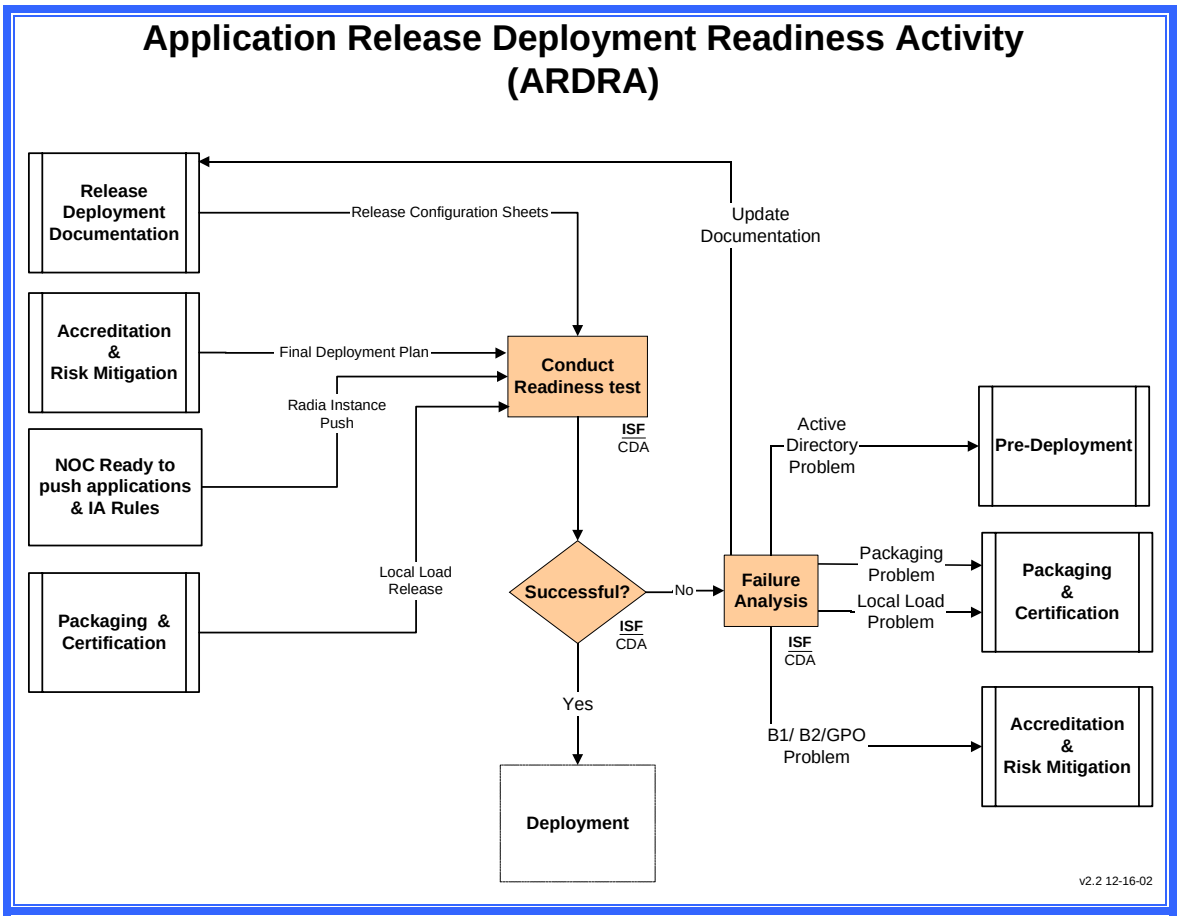


Figure 5-12 Application Release Deployment Readiness Activity (ARDRA)

5.10 RELEASE DEPLOYMENT PLAN (RDP)

The RDP provides a complete history of the release from inception to deployment. It contains all documentation used throughout the development and deployment processes to ensure informed decisions regarding the release are made. No detail is too small to be excluded from the plan if it has an impact on the release. CDA has sole responsibility for development and

maintenance of the plan. The CDA, ISF, and release sites will utilize this plan to manage the successful deployment of the release. A template for the RDP can be found in Appendix G of this guide and includes all pertinent information about the release and the following components:

- FAM Approval to Develop
- Request to Deploy approved by NETWARCOM
- General and Specific information pertaining to the release
- RFS
- Engineering Review Questionnaires (ERQ)
- POC information.
- Precertification Testing Results
  - IA results
- Release Information Collection
  - ATO
  - IATO
  - Licensing Information
  - Media
  - Identification of effected sites and users (UTAM)
  - Desktop and Server Connectivity Network Diagram
  - Installation Instructions
  - Test scripts/cases

All information pertaining to reengineering or fixes made to the release to satisfy testing and compliance requirements will be documented on the plan. If it is known that certain functions of the release will not work, these items shall be included in the plan.

CDAs are encouraged to use existing documents as part of the plan and should only create or capture information that has not been previously documented. The plan should be organized in a tabular format and stored in a three-ring binder. It is recommended that the RDP eventually become an automated document that is hosted on a web site available throughout the enterprise.

6.0 CONCLUSION

This guide fulfills the requirement for providing detailed information and guidance to application developers interested in migrating content, introducing new applications or changing existing applications within NMCI. The NRD^{2}G is written to support CDA in the development and deployment of releases that will operate within NMCI.

The NRD^{2}G is intended to be a work in progress with enhancements inserted as required to support the current state of NMCI implementation.

APPENDIX A: Glossary of Terms And Acronyms

A&RM	Accreditation and Risk Mitigation
AD	Active Directory
ADS	Authoritative Data Source
ADSI	Active Directory Service Interface
Agent Software	Any software that monitors and/or captures network traffic or queries network nodes for the purpose of reporting the captured information back to the user or another network node. This type of information is considered sensitive and its capture and dissemination poses a security risk.
AIS	Automated Information Systems
AIT	Application Integration and Testing
AOR	Assumption of Responsibility: The date when responsibility for operating the "as-is" environment and for work defined by the ordered NMCI CLINs shifts from the government and its local contractors to the Information Strike Force.
API	Application Program Interface
APLIT	Automated Post Local Installation Test
Application	(1) An automated software program that collects, stores, processes, and/or reports information in support of a specific user requirement. (2) Any software program that runs in a server-based or stand-alone environment that is used in a production capacity.
Application Development Software	Any software that generates or allows the user to create programming code which complies into executable (.exe) files that are installed and can be run from the user's workstation. Application Development Software is only permitted to reside on S&T seats.
Application Survey	The process of gathering COTS and GOTS application information necessary to rationalize or certify applications for migration to the NMCI environment. There are three categories of applications surveys: (1) desktop – a single user application not on the standard NMCI seat, (2) server-based, and (3) Web-based
ARDRA	Application Release Deployment Readiness Activity
ASN RDA	Assistant Secretary of the Navy for Research Development and Acquisition
ATO	Authority To Operate
B1	Boundary 1
B2	Boundary 2
B3	Boundary 3
B4	Boundary 4
BLII	Base Level Information Infrastructure

C&A	Certification and Accreditation: The comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. *Source: National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, National Information Systems Security (INFOSEC) Glossary.* Includes testing the ability of the application to electronically distribute.
CAL	Complex Application Laboratory
CCB	Change Control Board
CDA	Central Design Authority
CIO	Chief Information Officer
Client	The client part of *client-server architecture*. Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an *e-mail client* is an application that enables you to send and receive e-mail
CLIN	Contract Line Item Number
CM	Configuration Management
CNO	Chief of Naval Operations
COI	Communities of Interest
Common Portal Services	The logical set of common Portal functions and services exposed and available to the User Facing Service Developer
Content	The text, graphics, audio, video, services and applications available at a Web site.
COTS	Commercial Off the shelf
Cutover	The actual event of rolling out NMCI desktops. Cutover follows the preparation phases pre-AOR and post-AOR of the legacy applications transition. Cutover Start: In theory, Cutover begins at the pre-designated time when all pre-Cutover transition work is complete. Cutover actually begins upon the rollout of the first NMCI desktop at a site. Cutover Complete: In theory, Cutover is complete when the final desktop and application is successfully deployed. In actuality, Cutover ends at the successful rollout of the last scheduled desktop.
DAA	Designated Approval Authority
DADMS	Department of the Navy Application Database Management System
Deployment	The delivery of an authorized application to a designated server or desktop through an automated or local deployment process
DII COE	Defense Information Infrastructure Common Operating Environment
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DoD	Department of Defense
DON	Department of the Navy

DOS	Data Oriented Service: A software component that receives a request and optionally returns an XML Data Response. A Data-Oriented Service may interact with Common Portal Services and other Services published in the Service Registry.
DS	Directory Services
DST	Directory Services Team
DT&E	Developer Test and Evaluation
EAGLE	Enterprise Applications Group for Legacy and Emerging
ECCB	Enterprise Change Control Board
EDM	Enterprise Desktop Manager
EDS	Electronic Data Systems
Enterprise	Literally, a business organization. In the computer industry, the term is often used to describe any large organization that utilizes computers. An intranet, for example, is a good example of an enterprise computing system. In this case, the entire NMCI environment
ERQ	Engineering Review Questionnaire
ESO	Enterprise Solution Office
FAM	Functional Area Manager
FAQ	Frequently Asked Question
FDA	Functional Data Administrator
FDM	Functional Data Manager
FFP	Fleet Firewall Policy
FIFO	First In First Out
GOTS	Government Off the Shelf
GPO	Group Policy Object: a collection of settings that define what a system will look like and how it will behave for a defined group of users. GPO is associated with selected Active Directory containers, such as sites, domains, or organizational units (OUs).
HI	Horizontal Integration
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I&A	Identification and Authentication
IA	Information Assurance
IATO	Interim Authority to Operate
IATT	Information Assurance Tiger Team
IAVA	Information Assurance Vulnerability Alert
ID	Identification
IE	Internet Explorer
IM	Information Management
INFOSEC	Information Security

IP	Internet Protocol
ISF	Information Strike Force
IT	Information Technology
IT/IM	Information Technology / Information Management
IT-21	Information Technology for the 21st Century
Java	A general purpose, high-level, object-oriented, cross-platform programming language developed by Sun Microsystems [not an acronym]
JSP	Java Server Pages
LADRA	Legacy Application Deployment Readiness Activity
LATF	Legacy Applications Task Force
LATG	Legacy Application Transition Guide
LDAP	Lightweight Directory Access Protocol
Legacy Application	An existing customer software application that is not included in the NMCI standard seat services or the Contract Line Item Number (CLIN) 0023 catalog
Local Deployment	The act of manually loading an authorized client application to the NMCI seat.
LTSP	Lifecycle Technical Support Plan
MAC	Move, Add, Change
MCTN	Marine Corps Tactical Network
Metadata	Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. Metadata is essential for understanding information stored in data warehouses.
MS	Microsoft
MSI	Microsoft Windows Installer
NADTF	Navy Applications Database Task Force
NARMWG	NMCI Application Release Management Working Group
NAVNETWARCOM	Naval Network Warfare Command
NAVSEA	Naval Sea Systems Command
Navy IO	Navy Information Officer
NEP	Navy Enterprise Portal - The logical set of functional components that comprise the central portal infrastructure, including the Portal, the Service Registry and the Common Services. The gateway to the Navy Enterprise Portal is https://www.homeport.navy.mil/.
NETWARCOM	Naval Network Warfare Command
NIPRNET	Non-Secure Internet Protocol Router Network
NMCI	Navy Marine Corps Intranet
NOC	Network Operations Center
NOIS	Navy Ordering Information System
NRDDG	NMCI Release Development and Deployment Guide
NRMP	Navy Release Management Process

NRPM	NMCI Release Prioritization Manager
NRSM	NMCI Release Schedule Manager
OCONUS	Outside-Continental United States
OU	Organizational Units
PEO-IT	Program Executive Office for Information Technology
PIAB	Point of Presence-In-A-Box (PoP-in-a-Box): An engineering tool used by ISF to test applications for compatibility with the NMCI environment. The PoP simulates the NMCI environment and consists of Windows 2000 operating system, servers, and routers.
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POC	Point of Contact
POP	Point of Presence
POR	Program of Record
Portal	The functional component of the Navy Enterprise Portal that is responsible for aggregating Portlets.
Portal Client	A software application or hardware device that communicates with the Navy Enterprise Portal using the Portal Client Interface. Includes the set of web browsers, PDA's and mobile devices.
Portal Client Interface	An HTTP(s) Request\Response initiated by a Portal Client to the Navy Enterprise Portal.
Portal Service Response	A response sent from a Common Portal Service to a User-Facing Service
Portlet	The visible, active windows that end-users see within their Enterprise Portal interface.
PPL	Preferred Products List
RDP	Release Deployment Plan
RFC	Request for Change
RFS	Request for Service (DITCO)
RRPTE	Release in the Post Transition Environment
RTD	Request to Deploy
S&T	Science and Technology
Service Registry	The functional component of the Navy Enterprise Portal that stores metadata on User-Facing and Data-Oriented Services.
SGML	Standard Graphical Markup Language
SIPRNET	Secure Internet Protocol Router Network
SLA	Service Level Agreements
SM	Site Manager
SNAC	Systems and Network Attack Center

SOAP	Simple Open Access Protocol
SOC	Security Operations Center
SPAWAR	Space and Naval Warfare Systems Command
SSAA	System Security Authorization Agreement
SSL	Secure Socket Layer
TB	Transport Boundary
TFW	TFWeb, Task Force Web
TO	Task Order
UDDI	Universal Description Discovery and Integration
UNC	Universal Naming Convention
UPN	User Principal Name
URL	Uniform Record Locator
User Facing Service	A software component that receives a UFS Request from the Portal and returns an UFS Response that formats the content for display (usually in a markup language such as HTML or WML) to produce visual output in a Portlet. A User-Facing Service may interact with Common Portal Services and other Services published in the Service Registry
User Facing Service Request	A request sent to a User-Facing Service from the Navy Enterprise Portal. There are currently two types of User Facing Service Requests: HTTP Request and HTTP SOAP Request.
User Facing Service Response	A response sent to the Navy Enterprise Portal from a User-Facing Service.
USMC	United States Marine Corps
UTAM	User To Application Mapping
VBNS+	Very High Speed Backbone Network Service
VPN	Virtual Private Network
WAN	Wide Area Network
Web Service	A software component that is described via WSDL, can be published and located in a UDDI Registry, and invoked via SOAP over HTTP(s).
WIT	Waiver Input Template
WML	Wireless Markup Language
WSDL	Web Services Definition Language
WSE	Web Service Execution
WSEE	Web Service Execution Engine
WSRP	Web Services for Remote Portal
WWW	World Wide Web
XML	Extensible Markup Language. An extension/subset of Standard Graphical Markup Language (SGML) specifically designed for WWW dissemination and display of data. It is an open framework in which developers can develop

APPENDIX B: References

Useful Hyperlinks

Name	URL
General DoD Policy for Web Content	http://www.defenselink.mil/webmasters
DoD Mobile Code Policy	http://www.c3i.osd.mil/org/cio/doc/mobile-code11-7-00.html
INFOSEC Web Site	https://infosec.navy.mil
Public NMCI Web Site	http://www.nmci-isf.com/
OSD Deskbook Reference Library	http://web1.deskbook.osd.mil/htmlfiles/DBY_dod.asp
NMCI Transition	http://www.nmci-isf.com/transition.htm
DISA Information Systems Center (DISC)	http://www.disa.mil/disc/disc.html
Certified for Windows Program	http://msdn.microsoft.com/certification
DADMS	https://www.dadms.navy.mil
ISF Tools Database	http://www.nmci-isf.com/transition.htm#Legacy

Navy Messages #12

Originator	Message Date Time Group (DTG)	Subject
CNO WASHINGTON DC//N09T/N1/N2/N3/N4/N6/N7/N8/ N093/N095/N096//	R 252250Z FEB 02	NMCI LEGACY APPLICATIONS TRANSITION PROCESS//
PEO IT WASHINGTON DC//	R 261800Z FEB 02	ENTERPRISE LEGACY APPLICATION MANAGEMENT//
CNO WASHINGTON DC//N09T/N09W//	R 171442Z APR 02 NAVADMIN 007/01	NAVY ENTERPRISE PORTAL//
CINCPACFLT PEARL HARBOR HI//	R 301704Z NOV 01	NIPRNET PRIVATE WEB SERVER POLICY//
DIR NMCI & PMO//	R 242225Z MAY 02	NMCI PROCESS SUMMIT AGREEMENTS//
CNO WASHINGTON DC	R 232208Z MAY 02	ENTERPRISE STRATEGY FOR MANAGING APPLICATION DATABASES WITHIN THE NAVY
CNO WASHINGTON DC//N6N7//	R 301245Z SEP 02	ENTERPRISE STRATEGY FOR MANAGING NMCI APPLICATIONS AND DATABASES
CNO WASHINGTON DC//N6N7//	R 071718Z OCT 02	NAVY STANDARD APPLICATIONS
COMNAVNETWARCOM NORFOLK VA	R 131248Z DEC 02	SOFTWARE VERSION CONTROL

DoD Instructions

Instruction	Date	Subject
DoD5000.2-R	15 March 1996	Mandatory Procedures for Major Defense Acquisition Program (MDAPs) and Major Automated Information System (MAIS)

Instruction	Date	Subject
DoD 5200.28	21 March 1988	Security Requirements for Automated Information Systems (AISs)
DoD 5200.40	38 December 1997	DoD Information Technology Security Certification and Accreditation Process-DITSCAP
DoD 4630.5	11 January 2002	Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)

APPENDIX C: Points of Contact

NMCI Program Managers Office (PMO) POC List

NMCI PMO	POC	Billet	Email	Phone
PMO – Legacy Systems	Legacy Systems Division	Legacy Systems Division Director	peter.almazan@navy.mil	(858) 524-7435
PMO - EAGLE	EAGLE Team	EAGLE Lead	Joe.Dundas@navy.mil	(858) 537-8527
PMO - EAGLE	EAGLE Team	Development Approach Team Lead	lichtens@spawar.navy.mil	(619) 524-4546

NAVY CIO and NADTF POC List

NADTF	POC	Billet	Email	Phone
NADTF		Director	ron.sticinski@navy.mil	(202) 764-2942
NADTF		Member	judy.Kelly@navy.mil	(202) 764-1813
NADTF		Member	cynthia.corman@navy.mil	(202) 764-0852
NADTF		Member	warren.hedin@navy.mil	(202) 764-0012
CIO		Member	rodeck.renee@hq.navy.mil	(703) 604-6880
CIO		Member	Downing.Christine@hq.navy.mil	(703) 604-8390

Information Strike Force (ISF) POC List

ISF	POC	Email	Phone
Help Desk Phone			1-866-843-6624
AIT Manager		Kerry.Davis@eds.com	(619) 817-3453
AIT Sherman Street Lab Team Lead		tom.olson@eds.com	(619) 817-3866
AIT North Island NOC Lab		msmith08@eds.com	(619) 817-3526
PCL		tom.garity@eds.com	(619)-817-3536

All test applications and media submitted to the ISF AIT Certification Laboratory will be mailed to the following address:

EDS - NMCI/ISF/AIT
AIT Certification Lab
3970 Sherman Street
San Diego, CA 92110
Attn: Tom Olson

Legacy Applications POC liaisons
PMO - barnesbk@spawar.navy.mil 619-524-4557

USMC – smblatnmci@mcsc.usmc.mil 703-784-3134

For updates see https://tfw-opensource.spawar.navy.mil (under contacts) and http://www.nmci-isf.com/.

APPENDIX D: NMCI Application Ruleset (Revised)

V2.9.4

NMCI Ruleset is also posted on NADTF website
http://cno-n6.hq.navy.mil/navcio/leg_apps.htm

Ruleset Is A Reference	The NMCI Rule Set is designed to be a summary of the information contained in the Legacy Applications Transition Guide (LATG) and the NMCI Release Development and Deployment Guide (NRDDG). Should questions arise from the use of the Rule Set, the user should refer to the LATG, NRDDG or contact the Navy Applications Data Base Task Force (NADTF) for clarification.

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 1	**Windows 2000 (W2K) Compatible**	The candidate application is not compatible with the Windows 2000 operating system. This means it will either not run properly under Windows 2000 or that it interferes with the normal functionality of the operating system.	NAVY IO (NADTF) will not consider waivers of this Ruleset. Claimant must resolve the incompatibility by working with the application POR/CDA and owning FAM to upgrade the application to Windows 2000 compatibility or it should be replaced by another that is Windows 2000 compliant. Once compliant version is identified it will be submitted for NMCI testing and certification. Applications that cannot be corrected will be quarantined for no more than 6 months and then be removed from the quarantine workstation. The application will then be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel the RFS and unlink the application from their UICs in the ISF Tools database.	FAIL
RULE 2	**NMCI Group Policy Object (GPO) Compatible**	The candidate application is not compatible with the Group Policy Object (GPO) security rules for the workstation. For instance, if the candidate application requires full control of the c:\winnt folder in order to run, this violates NMCI enterprise policy governing connection to the NMCI network.	NAVY IO (NADTF) will not consider waivers of this Ruleset. Claimant must resolve the incompatibility by working with the application POR/CDA, owning FAM, ISF, IATT, and NMCI DAA in correcting the GPO failure. IATT or ISF will provide the technical data detailing cause of the failure. Once the GPO failure is resolved, the application will be re-tested. GPO Policy changes may be requested from the NMCI DAA. Applications that cannot be corrected will be quarantined for no more than 6 months and then be removed from the quarantine workstation. If the application cannot be corrected, then the application must be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	FAIL

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 3	**No Duplication of Gold Disk Software or Services**	The candidate application or service duplicates the functionality of the NMCI Standard Seat Services ("Gold Disk") application. (Example: Word 2000 replaces all versions of WordPerfect and other word processors. Windows Media Player, Real Player, and QuickTime replace all other audio/video players).	Claimant should discard the current application and use the application or service that exists on the Gold Disk. This application is not eligible for quarantine. Waiver requests may be submitted to NAVY IO (NADTF), but approvals will only be given if Claimant can show degradation to the mission, and can show they cannot afford to upgrade to authorized NMCI software or services. If the waiver is not approved or if no waiver is submitted, the application must be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application to their UICs in the ISF Tools database	KILL UNLESS WAIVER AUTHORIZED (NRFC)
RULE 4	**Comply with DON/NMCI Boundary 1 and 2 Policies**	The ISF or IATT have determined, through testing, that the candidate application is non-compliant with NMCI Boundary firewall policies (violation of B1/B2 Rulesets).	Claimant must resolve violation with the IATT, application POR/CDA, owning FAM, ISF, and NMCI DAA to determine how to correct the Boundary policy violation. Once the policy violation is resolved, the application will be re-tested. NAVY IO (NADTF) will not consider waivers of this Ruleset. Requests to operate a non-compliant system for B1 Firewall policy violations are managed by OPNAV and B2 policy changes are reviewed and managed by the NMCI DAA. B2 boundary issues may be resolved by moving servers into NMCI enclave. Applications that cannot be corrected will be quarantined for no more than 6 months and then be removed from the quarantine workstation. These applications will then be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	FAIL
RULE 5	**No Setup, Installation, Uninstallation, Update and Auto update Tools or Utilities**	The candidate application is actually a tool or utility used to load and remove application. Since ISF conducts all application installation and removal in NMCI, these types of files will not be authorized in ISF Tools DB or on the Rationalized List. Examples include Setup, Install, Uninstall, Launch, Autolaunch, Run, AutoRun, Updater, AutoUpdater or other installation type Applications	ISF will not test this application and NAVY IO (NADTF) will not consider waivers. These types of applications will be removed from tracking and the Legacy Applications Rationalized List and archived in the ISF Tools database. It will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	KILL (NRFC)

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 6	**No Games**	The candidate application is a "game" as defined by PEO-IT, NAVY IO and the PMO and is prohibited on the NMCI environment.	ISF will not test this application unless the POR/CDA, Echelon II and/or FAM determine the game is required for mission accomplishment (Modeling, Simulation, or Training). The Claimant must submit a waiver request to Navy IO (NADTF). Applications already approved by the M&S and/or Training FAM will not require waivers. If the waiver is not approved or if no waiver is submitted, the application must be removed from the Legacy Applications Rationalized List and archived in the ISF Tools database. It will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	**KILL UNLESS WAIVER AUTHORIZED (NRFC)**
RULE 7	**No Freeware or Shareware**	The candidate application is "Freeware" or "Shareware" as defined by PEO-IT, NAVY IO or the PMO and are prohibited in the NMCI environment. Enterprise life cycle support and licensing issues accompany most "Freeware".	Waivers for shareware will not be considered. Waivers for freeware will require an Echelon II, POR/CDA or FAM to generate a waiver request to NADTF. The waiver should include a request for the appropriate FAM to endorse the CDA, and will identify the CDA's willingness to support the application across the NMCI Enterprise. The NADTF will coordinate the waiver request with the NMCI DAA. Life cycle support and licensing issues for freeware must be resolved before they can be distributed to the Navy Enterprise. This application will not be installed on a quarantine workstation. If the waiver is not approved or if no waiver is submitted, the application must be removed from the Legacy Applications Rationalized List and archived in the ISF Tools database. The Echelon II commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	**KILL UNLESS WAIVER AUTHORIZED (NRFC)**
RULE 8	**No Beta/Test Software (Authorized on S&T Seats Only)**	The candidate application is a "beta" or a "test" version, as defined by the PEO-IT, NAVY IO, or the PMO and is therefore prohibited in the NMCI environment.	ISF will not test this application and the Navy IO (NADTF) will not consider waivers. These types of applications will not be tracked through the Legacy Application Transition process. These applications are not entered into the ISF Tools Database, not included on any rationalized list, nor should an RFS be submitted. If the Beta or Test Software is critical for mission accomplishment, the Claimant may purchase an S&T Seat. This application will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	**KILL (NRFC)**

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 9	**No Application Development Software (Authorized on S&T Seats Only)**	The candidate application is "application development" software, as defined by PEO-IT, NAVY IO-or the PMO, and therefore is not authorized on standard NMCI Seats. The candidate application would be permitted if operated on an NMCI ordered Science and Technology (S&T) Seat. Simple Application Development Software will not be tracked on the Rationalized List in the ISF Tools Database nor submitted for certification. Complex Application Development Software will require full NMCI testing and certification and will be tracked on the Rationalized List in the ISF Tools Database.	Simple Application Development Software will not be tested by ISF and the Navy IO (NADTF) will not consider waivers. These types of applications will not be tracked through-the Legacy Application Transition process. These applications are not entered into the ISF Tools Database, not included on any rationalized list, nor should an RFS be submitted. If the application development software is critical for mission accomplishment, the Claimant may purchase an S&T Seat, which allows for the installation of development software. This application will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application to their UICs in the ISF Tools database. Complex Application Development Software will be tested, certified, and deployed by the ISF and will tracked on the Rationalized List in the ISF Tools Database and will have an RFS submitted.	KILL (NRFC)
RULE 10	**No Agent Software**	The candidate application is "agent" software, as defined by PEO-IT, NAVY IO or the PMO. Agents in the NMCI environment are controlled by ISF. No other candidate agents are allowed in the NMCI environment. Agents are code modules installed on client machines (or network devices) often used to poll, monitor, and collect system or network node performance data and send it to management consoles elsewhere on the network. These present a security risk to NMCI. Network monitoring and management are the responsibilities of the ISF.	These types of applications will be removed from tracking in the Legacy Applications Rationalized List and the ISF Tools Database. NADTF will Kill these applications and waivers will not be considered. No polling and monitoring of legacy networks and systems and collecting of data is authorized from within NMCI Polling, monitoring and collecting system and network data of legacy networks and systems is still authorized from legacy network assets only. Viewing collected legacy network or system data from NMCI seats is allowed using non-agent software.	KILL (NRFC)

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 11	**Gold Disk Compatible**	The application software is not compatible with the standard "Gold Disk" software and services. This means that the candidate application does not interact properly with one or more of the set of applications or services that have been selected to be installed on all NMCI seats.	NAVY IO (NADTF) will not consider waivers of this Ruleset. The application is quarantined for no more than 6 months and then it is removed from the quarantine workstation. The application will be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel the RFS and unlink this application to their UICs in the ISF Tools database. Claimants and POR/CDA must work with the ISF to determine Gold Disk compatibility issues. The POR/CDA then works with the owning FAM to upgrade, replace or retire the application. Once a compliant version is identified it must be submitted for NMCI testing.	FAIL
RULE 12	**No Peripherals, Peripheral Drivers or Internal Hardware**	The candidate submission is a component (driver or hardware helper app) dealing directly with allowing a peripheral piece of hardware to function (Scanner, Printer, Plotters, Chartmakers, CDRW drive, ZIP or JAZ drive, Camcorder, PDA, etc). This enabling software must be tracked with the hardware on the Peripherals list and not entered into ISF Tools Database or listed on the Rationalized List. Internal hardware and the associated driver are not permitted within NMCI.	Peripherals and enabling software (drivers) are not entered into the ISF Tools Database nor placed on the Rationalized List. Peripherals and Peripheral Drivers are tracked separately from the ISF Tools Database and the Rationalized List, and are included in the Peripheral Drivers List. The Peripherals Drivers List is submitted to the ISF on-site for processing. If the driver is part of a bundled software package, that bundled package is handled like an application. The bundled package is entered into the ISF Tools Database, placed on the Rationalized List, and tested by the ISF.	KILL (NRFC)
RULE 13	**No personal, non-mission, or non-business related software**	The candidate application is "personal, non-mission, or non-business related", and is therefore prohibited in the NMCI environment.	ISF will not test this application unless the POR/CDA, Echelon II and/or FAM determine that this application is required for mission accomplishment. These applications will not be installed on a quarantine workstation. The claimant must submit a waiver request to Navy IO (NADTF). If the waiver is not approved or submitted, the application must be removed from the rationalized list and archived in the ISF Tools database Echelon II commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	KILL UNLESS WAIVER AUTHORIZED (NRFC)

RULE SET NUMBER	RULE NAME	RULE DESCRIPTION	OWNER REQUIRED ACTION	STATUS
RULE 14	**8/16-Bit Applications**	8-bit and 16-bit applications may migrate into the NMCI environment with an approved NAVY IO (NADTF) waiver, and a realistic migration plan that identifies a path to 32-bit status. Applications without approved waivers will not migrate to NMCI or Quarantined environments. Identification of an application as 8-bit or 16-bit does not stop the testing process (PIAB and LADRA). The application must pass all other rules and testing for 8-bit and 16-bit waivers to be approved.	Claimant and/or POR/CDA will submit a waiver immediately to NAVY IO (NADTF) requesting the 8/16-bit application migrate into NMCI. The request must include a detailed migration plan to get 8/16-bit application to 32-bit status. ISF must process and certify the application while the waiver is being submitted. ISF will hold the deployment of the application until waiver is authorized. If the waiver is not authorized (disapproved), the application is quarantined for no more than 6 months, then removed from the quarantine workstation and archived in the ISF Tools database. Applications for which a waiver was not submitted, will not be quarantined, will be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application to their UICs in the ISF Tools database.	PROCESS AND CERTIFY APPLICATION - HOLD FOR DEPLOYMENT UNTIL WAIVER AUTHORIZED

Definitions	
Fail	Fail is defined as an application that violates the NMCI Application Ruleset by failing to successfully meet compliance or usability testing standards. These applications are flagged as Quarantined and will operate on a quarantined workstation in the legacy environment until the Ruleset violation or test failure is resolved or a waiver to operate within NMCI has been submitted and approved.
Kill	Kill is defined as an application that violates the NMCI Application Ruleset. The application is not compliant with the rules and standards for applications within NMCI as set by the Navy IO. These applications will not be flagged as Quarantine and will be removed from the Rationalization List and ISF Tools database, unless a waiver to the rule is submitted and approved.
NRFC (Not Recommended For Certification)	NRFC is used by the ISF to designate any application that violates the NMCI Application Ruleset and will likely result in a Kill designation when reviewed by NADTF. Applications with an NRFC status have not been packaged or tested in the NMCI environment. This is an application that has not been processed by the ISF for violation of one or more of the following Rulesets: 3 – Duplication of Gold Disk 5 – No Setup Executables 6 - No Games 7 – No Freeware/Shareware 8 – No Beta Software 9 – No Development Software 10 – No Agent Software 12 – No Peripherals or Peripheral drivers 13 – No personal, non-mission, non-business software.
Application Development Software	Any software that generates or allows the user to create programming code which compiles into executable (.exe) files that are installed and can be run from the user's workstation. Application Development Software is only permitted to reside on S&T seats.
Agent Software	Any software that polls, monitors and/or captures network traffic or queries network nodes for the purpose of reporting the captured information back to the user or another network node. This type of information is considered sensitive and its capture and dissemination poses a security risk.

APPENDIX E: Factors and Issues for Application Migration

This section presents baseline factors and potential issues for applications migrating to the NMCI environment.

Factor	Issue
1. The NMCI user desktop is Windows 2000.	• Are desktop applications Windows 2000-compliant?
2. The NMCI desktop will be implementing Office 2000.	• Are there any interfaces to Office applications (Word, Excel) that might be affected by the Office 2000 implementation?
3. User desktops have dynamic TCP/IP addresses.	• Are there any issues with changing TCP/IP addresses at the desktop?
4. Servers moving into the NMCI network will have a different TCP/IP address assigned.	• Is there any hard coded logic based on TCP/IP addresses? • Is there hard code in script files, configuration files, parameters, and database entries? • Do external systems reference your server by TCP/IP address?
5. Printers within the NMCI network have a different naming scheme than currently used.	• Are there any hard coded printer names embedded in the application or application scripts? • Are there any unique desktop printing requirements (e.g., color, duplex, high speed, plotter, scanners, etc.)?
6. An NMCI user logs on to NMCI with a user ID that is different than the current user ID structure. For single sign-on NT domains, it may be more reasonable at this time (until the majority of users are transitioned) to prompt the user for the ID and password rather than creating a pass thru security mechanism.	• Are there hard coded tables that reference user IDs? • Are database permissions by user ID? • Are external interfaces sensitive to user ID?
7. NMCI users will be dialing into the NMCI dial-up servers. The TCP/IP address from the NMCI dial-up is different from that currently used.	• Do any issues relate to using a different dial-up facility than is currently in use? • Is anyone using PC/Anywhere or similar products?
8. A standard software configuration product locks the NMCI desktop down.	• Does the application install anything on the desktop? • Does the application install and uninstall properly in the Add/Remove program?
9. Is your application in compliance with the Navy Marine Corps Firewall Baseline Configuration?	•

Factor	Issue
10. Is all the desktop software available and configurable for standard software distribution?	•
11. If this application runs under an emulator, are there any anticipated issues (keyboard mapping) when the standard NMCI emulator (Reflections) is used?	•
12. Are there any other applications that interface with your application under NMCI?	• Does your application update any data used by another application? • Does your application run upstream or downstream from another application that it might effect? • Does your application share files, access shared files, or use drive mappings across workstations or servers? • Does the application depend on portable browser-initiated code? JavaScript and Java Applets are supported in the NMCI environment, but ActiveX components are not. Active X components used on the browser (client) for application access by users outside NMCI will not be allowed by the NMCI boundary. • Does the application rely on desktop plug-ins? • Does the application need any supporting applications (such as web browsers, ORACLE, PowerBuilder, 4th Dimension, runtimes)?
13. Does your application encrypt data during transmission or for storage? Does your application use encrypted data for input?	•
14. Users do not have administrative rights to their local machines.	• Developers must test applications with an account that does not have administrative rights.
15. The NMCI gold disk includes common desktop applications.	• As these applications may change over time, developers should develop to standard protocols and avoid the use of proprietary APIs.

APPENDIX F: NRD2G and Release Deployment Checklists

NRD2G Checklist

Checklists

Before We Get Started

- ☐ Develop communications plan
  - ☐ Education Plan/NRD^{2}G Road show
    - ☐ Architecture Overview (and CD) (ISF)
    - ☐ Benefits/Incentives/NMCI Intent (Govt.)
    - ☐ Lessons Learned
    - ☐ Highlight what developers can do and should not do
    - ☐ What we have today and where we're going tomorrow (view of 2.0).
- ☐ FAM Approval to develop and deploy

Before You Get Started

- ☐ Do you have a business process model?
- ☐ Does your application design take full advantage of the NMCI environment?
- ☐ Have you reviewed the NMCI CLINs available to your application?
- ☐ Have you reviewed the NMCI-ISF website?
- ☐ Have you laid out your operational and systems view?
- ☐ Have you assessed the impact of NMCI on your current application?
- ☐ Have you categorized your application (to include extranet/intranet)?
- ☐ Have you captured unique requirements based upon the categorization?
- ☐ Has your application been rationalized?
- ☐ What is the function of the application?
- ☐ Have you coordinated with the application owner?
- ☐ Do you have clearance from the data owner to use the data?
- ☐ Does your application have sufficient funding?
- ☐ Have you developed a data model?
- ☐ Have you obtained the appropriate authority sign-offs for your business process model, data model, rationalization, etc.?
- ☐ Do you have your licenses?
- ☐ Do you have your acquisition documentation?
- ☐ Have you obtained your MDA certification?
- ☐ Have you reviewed the firewall policies?
- ☐ Have you determined whether the application will be hosted by NMCI or maintained by the Command/Claimant?

When You Develop Your Application

- ☐ Have you acquired an NMCI development environment?
- ☐ Do you understand the restrictions that NMCI places on your application development (Windows 2000, Group Policy Object Settings, desktop & user account lockdowns, Registry editing, Directory permissions, etc)?

Before You Visit NMCI For An Engineering Review

- ☐ Have you completed your certification and accreditation (CNA) package?
- ☐ Do you have a network topology of your application that shows interfaces and ports?
- ☐ Have you completed all of your testing?
- ☐ Have you invited the application owner/developer owner to the review?
- ☐ Have you invited the local DAA?

Before You Go Into The Certification Lab

- ☐ Have you reviewed the Justification ID's for CBNR, NRFC & Failed Materials? (Certified But Not Recommended, Not Recommend For Certification)
  Do you have your test plans and scenarios?
- ☐ Have you completed your RFS with installation instructions?
- ☐ Have you scheduled your certification with the lab?
- ☐ Has the application been previously certified?

When You Go Into The Certification Lab

- ☐ For PIAB (portable NMCI, backend servers, active directory, firewall policy), do you have resources (facilities, testers) available?

Before You Deploy/Migrate

- ☐ Have you completed your NCAP? (NMCI connection approval process)
- ☐ Have you trained your users?
- ☐ Do you have your Help Desk procedures in place?
- ☐ Is the NMCI Help Desk prepared for your application?
- ☐ Do you have adequate backup and disaster recovery plans?

When You Deploy/Migrate

- ☐ Is the NMCI Help Desk aware of your application's Help Desk?
- ☐ Have you exchanged handoff information with the Help Desk?
- ☐ Are updates to your applications scheduled?
- ☐ Are you updating the ISF Help Desk as incidents/changes occur?
- ☐ Is proper ticketing and incident management taking place?
- ☐ Is the knowledge base being updated?

NRD2G Checklist

Getting Started

☐ Develop a Release Deployment Plan:

- ☐ Write a Deployment Strategy
- ☐ Identify which sites will use the release
- ☐ Diagram a Server and User Mapping
- ☐ Write a Training Strategy
- ☐ Developed/update the Network Diagram
- ☐ Write/forward the installation instructions
- ☐ Collect and forward the licensing information
- ☐ Write and forward the test scripts/cases
- ☐ Compile ATO, IATO and DITSCAP documentation
- ☐ Complete Engineering review questionnaires
- ☐ Write Precertification results

☐ Seek approval if Emergency/Urgent Release.
☐ Obtain specific submission window from the AIT lab (if unknown).
☐ Submit the release to the AIT lab in the submission window.

Testing the Release

☐ Obtain a copy of the NMCI Gold Disk from the AIT lab.
☐ Test the release for Windows 2000 and NMCI Gold Disk compliance.
☐ Test for Information Assurance (IA) compliance (B1, B2, and GPO).
☐ Document non-compliant release information for the waiver process.

Before Certification

☐ Obtain formal written approval from the ECCB.
☐ Capture Precertification information:

- ☐ Obtain release licenses.
- ☐ Identified desktops and server connectivity in network diagram.

- ☐ Updated release deployment plan
- ☐ Compile IA results (ports, protocols, and services).

Submitting The Release & Documentation

- ☐ Generate a CDA Request for Service (RFS) on the ISF Tools Database.
- ☐ Provide installation instructions, media, licenses, and detailed test scripts.
- ☐ Provide existing ATO, IATO and DITSCAP documentation (Annual Releases).
- ☐ Complete an ERQ (Annual Releases).

During Certification

- ☐ Participate in testing the release (Packaging Lab, if required).
  a. ☐ Check the ISF Tools Database to discover any packaging problems.
  b. ☐ Work with AIT Lab to perform Quick Fixes, if needed.

Final Verification

a. ☐ Perform an ARDRA, if planned.
b. ☐ Verify user rights in the Active Directory.
c. ☐ Assist Site Manager in the release push to the desktops.

APPENDIX G: Release Deployment Plan

NMCI Release Deployment Plan

INTRODUCTION

The NMCI Release Deployment Plan (NRDP) is an essential part of the NMCI Release Deployment Process to introduce a release into the NMCI environment. The NMCI Release Development and Deployment Guide (NRD²G) supports the CDA by providing information that is essential for a release to meet all DON and NMCI programming requirements. The CDA is responsible for the development and maintenance of this plan. It will document all aspects of planning, development, deployment, and will provide pertinent information to other government, contractor and ISF personnel having a role in the process. The plan is a management tool to assist the CDA in ensuring that all required actions are completed and to provide quality assurance to document problem areas and solutions.

COMMUNICATIONS PLAN

The overall success of this plan will depend on the ability of the CDA to effectively communicate with all parties that have a role in the process. This includes the users, sites, Functional Area Manager (FAM), Echelon II (ECHII), developers and the ISF. From the beginning the CDA must ensure that the activity requesting the release is getting what was requested as approved by the FAM and ECHII command. Once the release has been submitted for certification and deployment, the CDA must be actively engaged with ISF Application Implementation and Testing (AIT) laboratory and Complex Application Laboratory (CAL) facility to respond to and resolve problems as they occur during the Packaging, Certification and Testing processes. This will ensure that the release completes the processes and is deployed within the time period specified in the submission window. The CDA will create a detailed POC listing of all activities and agencies that have a role in the process. Insert the POC Listing as the last TAB in the plan using the following format:

Name	Command/Company	Phone Number	E-Mail Address

Note: DON't wait until the last minute to check on the status of your release.

RELEASE INFORMATION

a. Application Information:

1. NAME OR TITLE:
2. ACRONYM:
3. VERSION NUMBER:
4. BUILD NUMBER (IF APPLICABLE):
5. FUNCTIONAL AREA:

b. Classification of the Application:

c. Application Central Design Authority (CDA) POC Information:

1. NAME:
2. COMMAND:
3. CODE/DIVISION:
4. COMMERCIAL PHONE NUMBER:
5. DSN PHONE NUMBER:
6. E-MAIL ADDRESS:
7. CDA PARENT SITE/COMMAND NAME AND UIC:

d. CDA Echelon II Command:

1. LIST #1:
2. LIST #2:

e. Application Program of Record (POR) or Program Manager (PM) or Point of Contact (POC) Information:

1. NAME:
2. COMMAND:
3. COMMERCIAL PHONE NUMBER:
4. DSN PHONE NUMBER:

5. E-MAIL ADDRESS:
6. TYPE: ☐ POR ☐ PM ☐ POC

f. Number of Users for this release:

g. Type of release:

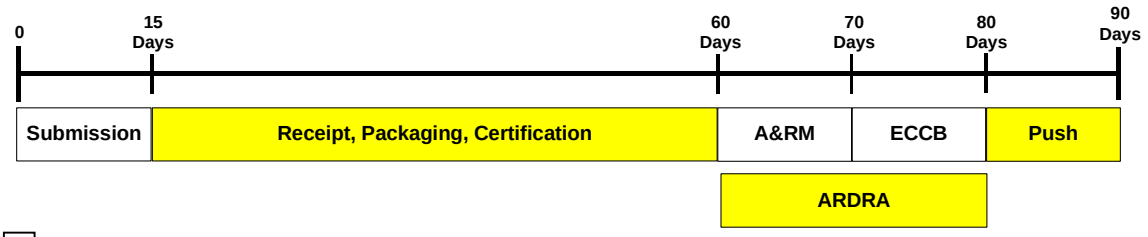
h. Does this release or new application interact or depend on another application? ☐ Yes ☐ No. If yes, provide the following information:

1. APPLICATION NAME:
2. APPLICATION ACRONYM:
3. APPLICATION VERSION:
4. CLASSIFICATION OF THE APPLICATION:
5. APPLICATION POC:
   A) NAME:
   B) COMMAND:
   C) CODE/DIVISION:
   D) COMMERCIAL PHONE NUMBER:
   E) DSN PHONE NUMBER:
   F) E-MAIL ADDRESS:

Does the application require a waiver?

TYPE OF SUBMISSION WINDOW

The following timeline must be followed to ensure that adequate time is provided for the release to complete the NMCI Release Deployment Process. Select the submission window type for this release from the options below. A complete explanation of each step in the process is provided in the NRD²G.



☐ Annual Release

☐ Planned Point Release (quarterly)

☐ Emergency/Urgent Release (must be approved by ECCB)

RELEASE CONFIGURATION

How is the release configured to operate on the workstation?

☐ Client

☐ Client/Server

☐ Server Based

☐ Web-enabled

REQUEST FOR CHANGE (RFC)

A copy of the completed RFC must be attached to the plan to document the reason and approval of the release. Has this release been approved for development by the FAM and Echelon II command? ☐ Yes ☐ No.

If no, no further action should be taken until approval and funding has been granted.

Attach a copy of the RFC as TAB A of the Release Deployment Plan.

Provide additional comments as necessary:

Comments:

CDA REQUEST FOR SERVICE (RFS)

All releases must be registered into the ISF Tools database and have a completed RFS. The template for an RFS is available at the www.nmci-isf.com/transition/html.

Has the release been registered in the ISF Tools database? ☐ Yes ☐ No.

If yes, insert the RFS Number and attach a copy of the RFS as TAB B of the Release Deployment Plan.

If no, the CDA must complete and submit an RFS to the ISF.

Provide additional comments as necessary:

Comments:

PRECERTIFICATION

Has the release gone through the Precertification process? ☐ Yes ☐ No.

If yes, did the release successfully pass Precertification? ☐ Yes ☐ No.

If no to any of the above questions, continue Precertification until the application has successfully passed and is ready for deployment. Attach a copy of the Precertification results as TAB D of the Release Deployment Plan.

Provide additional comments as necessary:

Comments:

ENGINEERING REVIEW QUESTIONNAIRE (ERQ)

All Annual Releases will require a completed ERQ. Has an ERQ been completed for this release ☐ Yes ☐ No.

If No, the CDA must complete an ERQ and submit it with the release to the ISF.

Attach a copy of the completed ERQ as TAB D of the Release Deployment Plan:

Comments:

INTERIM AUTHORITY TO OPERATE (IATO)/AUTHORITY TO OPERATE (ATO)

Does the release have an existing IATO or ATO? ☐ Yes ☐ No.

If yes, what type of the authority to operate does it have? ☐ IATO ☐ ATO. Attach a copy of the selected document as TAB D to the Release Deployment Plan.

Comments:

HOSTING REQUIREMENTS

Any special hosting requirements should be identified prior to Precertification.

Does the CDA intend to host their release? ☐ Yes ☐ No.

If yes, is CLIN 00027 required for connectivity? ☐ Yes ☐ No.

If no, does the CDA intend to exercise CLIN 00029? ☐ Yes ☐ No.

If CLIN 00027 or 00029 is exercised, attach a copy of the request in TAB E of the Release Deployment Plan.Provide additional comments as necessary:

Comments:

TRAINING

The CDA is responsible for developing and funding any training required to support the deployment and use of a release or new application.

Is there training required to support this release or new application: ☐ Yes ☐ No.

If yes, has a training plan been developed: ☐ Yes ☐ No.

If yes, attach a copy of the Training Plan to TAB F of the Release Deployment Plan.

> If no, complete and attach the Training Plan prior to deployment in TAB F of the Release Deployment Plan.

Provide additional comments as necessary:

Comments:

NETWORK DIAGRAM

RELEASE CHANGES

It is essential to keep a record of all changes made to a release to maintain and satisfy testing and certification requirements. This information will provide a roadmap of the

release journey and is an excellent source of information for future release development. This information will be captured in the table below.

Process	Error	Solution

TYPE OF DEPLOYMENT

The ISF, with the CDA, will determine the type of deployment to be used based on the results of the Packaging and Certification Audit process. Select the deployment option to be used for distribution of this release:

- ☐ Push
- ☐ Local Deployment

APPENDIX H: Navy Functional Area Manager List

FUNCTIONAL AREA	ACTIVITY	FAM	E-MAIL ADDRESS	PHONE NUMBER
ACQUISITION	ASN (RD&A)	RADM Robert Cowley	Cowley.robert@hq.navy.ml	703 602-2338
ADMINISTRATION	OPNAV N1	VADM Patricia Tracey	travey.patricia@hq.navy.ml	703 692-9084
CIVILIAN PERSONNEL	ASN (M&RA)	Mr. Lawrence West	lawrence.west@navy.mil	202 764-0820
COMMAND, CONTROL & COMM	OPNAV N6/N7	RADM Thomas Zelibor	Zelibor.thomas@hq.navy.mil	703 614-2042
FINANCIAL MANAGEMENT	ASN (RD&A)	Mr. Ed Johnson	Johnson.edward@fmo.nav.mill	
INFORMATION WARFARE	OPNAV N6/N7	RADM Thomas Zelibor	Zelibor.thomas@hq.navy.mil	703 614-2042
INTELLIGENCE & CRYPTOLOGY	OPNAV N2	RADM Richard Porterfield	Porterfield.richard@hq.navy.mil	703 614-0281
LEGAL	GC	Dr. Michael Bowman	michael.bowman@navy.mil	
LOGISTICS	OPNAV N4	Ms. Ariane Whittemore	Whittemore.ariane@hq.navy.mil	703 693-7651
MANPOWER & PERSONNEL	OPNAV N1	Mr. Matt Henry	N1B@bupers.navy.mil	703 614-1101
MEDICAL	OPNAV N093	VADM Michael Cowan	MLCowan@us.med.navy.mil	
METEROLOGY & OCEANOGRAPHY	OPNAV N096	RADM Tom Donaldson	DonaldsonT@CNMOC.navy.mil	
MODELING & SIMULATION	OPNAV N6/N7	RADM Thomas Zelibor	Zelibor.thomas@hq.navy.mil	703 614-2042
NAVAL NUCLEAR PROPULSION	OPNAV NOON	Mr. Jim Mosquera	Mosquerajp@navsea.navy.mil	
PRECISE TIME & ASTROMETRY	OPNAV N096	CAPT Dave Gillard	gillard.dave@usno.navy.mil	
READINESS	OPNAV N4	Ms. Ariane Whittemore	Whittemore.ariane@hq.navy.mil	703 693-7651
RELIGIOUS MINISTRIES	OPNAV N097	RADM Barry Black	Black.barry@hq.navy.mil	
Res, Rqmt & ASSESSMENTS	OPNAV N8	Ms. Bonnie Morehouse,	Morehouse.bonnie@hq.navy.mil	
RESERVE AFFAIRS	OPNAV N095	RADM Craig McDonald	McDonald.Craig@hq.navy.mil	703 601-1810
SCIENTIFIC & TECHNICAL	OPNAV N091	CAPT Thomas Gardner	Gardner.thomas@hq.navy.mil	703 601-1729
TEST & EVALUATION	OPNAV N091	CAPT Steve Shegrud	Shegrud.Stevens@hq.navy.mil	703 601-1733
TRAINING & EDUCATION	OPNAV N79	Dr. Allen Zeman	Zeman.allen@hq.navy.mil	703 692-9827
WEAPONS PLANNING & CONTROL	OPNAV N6/N7	RADM Thomas Zelibor	Zelibor.thomas@hq.navy.mil	703 614-2042

APPENDIX I: Samples, Examples and Templates

This appendix will provide various samples, examples, and templates for use by CDAs as part of documenting, developing, and deploying releases.

Tab 1 Sample Test Script
Tab 2 Example Installation Instruction
Tab 3 Example User to Application Mapping Template
Tab 4 DII COE Templates

APPENDIX I, Tab 1: Sample Test Script

Sample Test Script

This is an example of test cases and procedures used by the ISF to test the proper installation and functionality of the software.

Generating SQL Scripts for SMS Views

The information in this article applies to:

- Microsoft Systems Management Server 1.1
- Microsoft Systems Management Server 1.2

This article was previously published under Q133253

Summary

SMSVIEW creates various views that can be used when querying the Systems Management Server SQL Database. The SQL Scripts used to create these views can be dumped using Microsoft SQL Enterprise Manager (in Microsoft SQL Server 6.0).

More Information

To generate the SQL scripts to create the SMS views:

1. Start SQL Enterprise Manager.
2. If the server where the Systems Management Server database resides is not already registered in SQL Enterprise Manager, register it as follows:
    1. Select Register Server from the Server menu.
    2. Provide the server name and valid logon information (by default, the valid logon is SA with no password and Standard Security).
    3. Choose Register.
3. In the Server Manager window, select the server you just registered (there may be a slight delay as a connection to this server is established).
4. Choose + in the following order:
    1. The Server's name in the Server Manager window.

2. Databases to get to the Systems Management Server database.

3. The database that contains the Systems Management Server data.

The name of the SMS database in the Server Manager window should be selected.

5. Select Generate SQL Scripts from the Object menu.

6. In the Generate SQL Scripts - <servername>\<database name> dialog box, choose All Views for Scripting Objects. This fills in the name of each view in the list box at the bottom right portion of the dialog box.

7. Ensure Object Creation and Object Drop are selected for Scripting Options.

8. If you prefer scripts for each view to be placed in a separate file, select Per Object in Scripting Options. Otherwise, select Single File.

9. Choose Preview (there is a short wait as the scripts are generated). Save the scripts as text files or choose Close to go back to the Generate SQL Scripts dialog box without saving the scripts).

The following displays the resulting output (in Systems Management Server 1.1, Build 682):

```
/****** Object:  View dbo.vDisk    Script Date: 7/5/95 4:30:43 AM ******/
if exists (select * from sysobjects where id = object_id('dbo.vDisk') and

sysstat & 0xf = 2)
drop view dbo.vDisk

GO

Create View vDisk as select dwMachineID , Disk_SPEC.__Disk_Full0 ,
Disk_COMM.Disk_Index0 , Disk_COMM.File_System0 ,
Disk_SPEC.Free_Storage__MByte_0 , Disk_SPEC.Sectors0 ,
Disk_SPEC.Serial_Number0 , Disk_SPEC.Storage_Size__MByte_0 ,
Disk_COMM.Storage_Type0 , Disk_SPEC.Storage_Used__MByte_0 ,
Disk_SPEC.Volume_Name0 from  MachineDataTable  ,Disk_COMM   , Disk_SPEC
where Disk_COMM.datakey =*  CommonKey and Disk_SPEC.datakey =* SpecificKey
and ArchitectureKey = 5 and GroupKey = 8

GO

/****** Object:  View dbo.vEnvironment    Script Date: 7/5/95 4:30:43 AM
******/
if exists (select * from sysobjects where id =
object_id('dbo.vEnvironment')
```

```
and sysstat & 0xf = 2)
drop view dbo.vEnvironment

GO

Create View vEnvironment as select dwMachineID ,
Environment_SPEC.Environment_String0 , Environment_SPEC.Value0 from
MachineDataTable  ,Environment_COMM   , Environment_SPEC where
Environment_COMM.datakey =*  CommonKey and Environment_SPEC.datakey =*
SpecificKey and ArchitectureKey = 5 and GroupKey = 12

GO

/****** Object:  View dbo.vGroupNames    Script Date: 7/5/95 4:30:44 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vGroupNames')
and sysstat & 0xf = 2)
drop view dbo.vGroupNames

GO


Create View vGroupNames as select  GM.GroupName   FROM ArchitectureMap AM,
GroupMap GM  WHERE  GM.ArchitectureKey = AM.ArchitectureKey AND
((AM.Mode=0))

GO

/****** Object:  View dbo.vIdentification    Script Date: 7/5/95 4:30:44 AM
******/
if exists (select * from sysobjects where id =
object_id('dbo.vIdentification') and sysstat & 0xf = 2)
drop view dbo.vIdentification

GO

Create View vIdentification as select dwMachineID ,
Identification_SPEC.Domain0 , Identification_SPEC.LogOn_Name0 ,
Identification_SPEC.Name0 , Identification_SPEC.NetCardID0 ,
Identification_SPEC.Site0 , Identification_SPEC.SMSID0 ,
Identification_SPEC.SMSLocation0 , Identification_SPEC.SystemRole0 ,
Identification_SPEC.SystemType0 from  MachineDataTable
,Identification_COMM

, Identification_SPEC where Identification_COMM.datakey =*  CommonKey and
```

```
Identification_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 1

GO

/****** Object:  View dbo.vMouse    Script Date: 7/5/95 4:30:44 AM ******/
if exists (select * from sysobjects where id = object_id('dbo.vMouse') and
sysstat & 0xf = 2)
drop view dbo.vMouse

GO

Create View vMouse as select dwMachineID , Mouse_COMM.Hardware_Installed0 ,
Mouse_COMM.Language0 , Mouse_COMM.Manufacturer0 ,
Mouse_COMM.Mouse_Hardware_Type0 , Mouse_COMM.Number_of_Buttons0 from
MachineDataTable  ,Mouse_COMM   , Mouse_SPEC where Mouse_COMM.datakey =*
CommonKey and Mouse_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 4

GO



/****** Object:  View dbo.vNetcard    Script Date: 7/5/95 4:30:45 AM
******/

if exists (select * from sysobjects where id = object_id('dbo.vNetcard')
and


sysstat & 0xf = 2) drop view dbo.vNetcard

GO

Create View vNetcard as select dwMachineID , Netcard_SPEC.IRQ0 ,
Netcard_COMM.Manufacturer0 , Netcard_SPEC.Port_Address0 from
MachineDataTable  ,Netcard_COMM   , Netcard_SPEC where Netcard_COMM.datakey
=*  CommonKey and Netcard_SPEC.datakey =* SpecificKey and ArchitectureKey =
5 and GroupKey = 11

GO

/****** Object:  View dbo.vNetwork    Script Date: 7/5/95 4:30:45 AM
******/

if exists (select * from sysobjects where id = object_id('dbo.vNetwork')
```

```
and



sysstat & 0xf = 2) drop view dbo.vNetwork

GO

Create View vNetwork as select dwMachineID , Network_COMM.Default_Gateway0
,

Network_SPEC.IP_Address0 , Network_SPEC.IPX_Address0 ,
Network_COMM.LogOn_Name0 , Network_COMM.Major_Version0 ,
Network_COMM.Minor_Version0 , Network_SPEC.Network_Active0 ,
Network_COMM.Network_Type0 , Network_COMM.Subnet_Mask0 from
MachineDataTable  ,Network_COMM   , Network_SPEC where Network_COMM.datakey
=*  CommonKey and Network_SPEC.datakey =* SpecificKey and ArchitectureKey =
5 and GroupKey = 10

GO




/****** Object:  View dbo.vOperating_System    Script Date: 7/5/95 4:30:45
AM ******/
if exists (select * from sysobjects where id =

object_id('dbo.vOperating_System') and sysstat & 0xf = 2)
drop view dbo.vOperating_System

GO

Create View vOperating_System as select dwMachineID ,

Operating_System_COMM.Build_Number0 , Operating_System_COMM.Build_Type0 ,
Operating_System_COMM.Country_Code0 ,
Operating_System_SPEC.Installation_Date0 ,
Operating_System_COMM.Language_ID0 ,
Operating_System_COMM.Operating_System_Name0 ,
Operating_System_COMM.Registered_Organization0 ,
Operating_System_SPEC.Registered_Owner0 ,
Operating_System_SPEC.System_Root0

, Operating_System_SPEC.System_Start_Options0 ,
Operating_System_COMM.Version0 from  MachineDataTable
,Operating_System_COMM   , Operating_System_SPEC where
```

```
Operating_System_COMM.datakey =*  CommonKey and
Operating_System_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 7

GO

/****** Object:  View dbo.vPC_Memory    Script Date: 7/5/95 4:30:46 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vPC_Memory')
and sysstat & 0xf = 2)
drop view dbo.vPC_Memory

GO

Create View vPC_Memory as select dwMachineID ,
PC_Memory_SPEC.Page_File_Name0 , PC_Memory_SPEC.Page_File_Size__MByte_0 ,
PC_Memory_SPEC.Total_Paging_File_Space__0 ,
PC_Memory_SPEC.Total_Physical_Memory__KB0 from  MachineDataTable
,PC_Memory_COMM   , PC_Memory_SPEC where PC_Memory_COMM.datakey =*
CommonKey and PC_Memory_SPEC.datakey =* SpecificKey and ArchitectureKey = 5
and GroupKey = 9

GO

/****** Object:  View dbo.vProcessor    Script Date: 7/5/95 4:30:46 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vProcessor')
and sysstat & 0xf = 2)
drop view dbo.vProcessor

GO

Create View vProcessor as select dwMachineID ,
Processor_COMM.Processor_Name0 , Processor_COMM.Processor_Type0 ,
Processor_COMM.Quantity0 from  MachineDataTable  ,Processor_COMM   ,
Processor_SPEC where Processor_COMM.datakey =*  CommonKey and
Processor_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 6

GO

/****** Object:  View dbo.vServices    Script Date: 7/5/95 4:30:46 AM
******/
if exists (select * from sysobjects where id = object_id('dbo.vServices')
and sysstat & 0xf = 2)
drop view dbo.vServices
```

```
GO

Create View vServices as select dwMachineID , Services_SPEC.EXE_Path0 ,
Services_COMM.Name0 , Services_SPEC.Start_Name0 , Services_COMM.Start_Type0
, Services_COMM.State0 from  MachineDataTable  ,Services_COMM   ,
Services_SPEC where Services_COMM.datakey =*  CommonKey and
Services_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 13

GO

/****** Object:  View dbo.vVideo    Script Date: 7/5/95 4:30:47 AM ******/
if exists (select * from sysobjects where id = object_id('dbo.vVideo') and

sysstat & 0xf = 2)
drop view dbo.vVideo

GO

Create View vVideo as select dwMachineID , Video_COMM._nd_Adapter_Type0 ,
Video_COMM.Adapter_Type0 , Video_SPEC.Bios_Date0 ,
Video_COMM.Current_Video_Mode0 , Video_COMM.Display_Type0 ,
Video_COMM.Manufacturer0 , Video_COMM.Max_Rows0 from  MachineDataTable
,Video_COMM   , Video_SPEC where Video_COMM.datakey =*  CommonKey and
Video_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and GroupKey = 5

GO

/****** Object:  View dbo.vWorkstationStatus    Script Date: 7/5/95 4:30:47
AM ******/
if exists (select * from sysobjects where id =
object_id('dbo.vWorkstationStatus') and sysstat & 0xf = 2)
drop view dbo.vWorkstationStatus

GO

Create View vWorkstationStatus as select dwMachineID ,
WorkstationStatus.Failed_Hardware_Checks0 ,
WorkstationStatus.Files_Not_Installed0 , WorkstationStatus.LastHWScan ,
WorkstationStatus.LastSWScan , WorkstationStatus.Standalone_Workstation0 ,
WorkstationStatus.System_Files_Not_Modified0 from  MachineDataTable  ,
WorkstationStatus where WorkstationStatus.datakey =* SpecificKey and
ArchitectureKey = 5 and GroupKey = 2

GO
```

APPENDIX I, Tab 2: Example Installation Instruction

The following is an example of an installation instruction that the ISF will use to install the release for testing.

Visio2000: Revised Network Installation Instructions (Network.wri) for
Visio 2000 Standard Edition

The information in this article applies to:
Microsoft Visio 2000 Standard Edition
This article was previously published under Q258467

SUMMARY

The Network.wri file that is included with Microsoft Visio 2000 Standard Edition contains incorrect instructions for how to perform a network installation.

This article contains the full text of the Network.wri file, with the corrections incorporated. Use the information in this article instead of the Network.wri file when you need to do either of the following:

Install Visio 2000 Standard Edition to a network drive for shared use.
-or-
Install Visio 2000 Standard Edition locally from a network drive.

MORE INFORMATION

Visio® 2000 Standard Edition
Network Installation Instructions

File version 6.0.0 Visio(R) 2000 Standard Edition US English version
Network Installation Instructions

This file contains information about setting up and running Visio 2000 on a network. We recommend that you read this file and keep a printed copy with your Visio documentation. For other late-breaking information about installing and running Visio 2000, see the README.WRI file. For a list of all the files copied to your hard drive if you install the complete version of Visio 2000, see the FILELIST.WRI file.

CONTENTS

1. NETWORK LICENSING INFORMATION

To run Visio on a network that gives more than one-person access to the product, you need to acquire additional licenses either by purchasing additional retail packages of Visio or by purchasing license packs.

A license pack, which authorizes one additional user, includes a product license, a serialized registration card, and a documentation order form.

2. OPERATING SYSTEM REQUIREMENTS FOR VISIO 2000

To use Visio 2000 Standard Edition, you must be running one of the following 32-bit Microsoft Windows operating systems:

- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT 4.0 (Service Pack 3 or later is required)

Service Packs for Windows 95, Windows 98, and Windows NT operating systems can be obtained from Microsoft Corporation (www.microsoft.com).

NOTE: To install Visio 2000 on a workstation running Windows NT 4.0, the user installing the product must have Administrator privileges for that workstation.

NOTE: Installation Path Length Limitation: To ensure operation of the Visio 2000 Solutions the directory chosen for installation of Visio 2000 Standard Edition must have a path name of less than 55 characters in length.

3. NETWORK SETUP OVERVIEW

Setting up Visio on a network is a two-step process: First, you install Visio on the network server; second, you set up individual workstations so they can run Visio from the server or from each workstation's hard disk.

NOTE: Setting up Visio 2000 on a network server for shared use requires Windows NT 4.0 SP 3 or later. This procedure is not supported under Windows 95 or Windows 98. For details about setting up Visio on a network so that multiple workstations can use a shared copy from the server, see "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE" below.

For details about setting up Visio files on a network server so that the program can be loaded onto the hard disks of individual workstations, see "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR LOCAL INSTALLATION TO WORKSTATIONS" below.

4. PREPARING A WORKSTATION TO SET UP VISIO FOR SHARED USE

The Visio 2000 setup program is based on the Microsoft Windows Installer (MSI) technology. MSI must be installed on the workstation you are using to set up Visio 2000 for shared use before starting the Visio 2000 setup program. If MSI is not installed on the workstation, or if you are in doubt, use the following procedure to install MSI:

1. Insert the Visio 2000 CD into your CD-ROM drive.
2. From the Start menu, choose Run.
3. Type d:\Install\bin\sp\MSI\WinNT\InstMSI, where d is the letter assigned to your CD-ROM drive.

After installing MSI, complete the following procedure to install Visio 2000.

5. SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE

To install Visio 2000 on a network server for shared use:
You must have write access to the network server to install Visio on the server.

NOTE: Do not run the Setup.exe file located in the root directory of the Visio CD for this procedure. This file is for single-user installations only, and will not install Visio correctly for shared use.

1. From a workstation running Windows NT 4.0, log on to the network and connect to the drive where you want to install the Visio program.
2. Insert the Visio 2000 CD into your CD-ROM drive.
3. From the Start menu, choose Run.
4. Type d:\Install\Setup /a where d is the letter assigned to your CD-ROM drive.
   Setup prompts you for the location of your Visio installation.
5. Type e:\visio, where e is the letter assigned to the network server and Visio is the directory on the server where the Visio program files will reside.
6. Follow the instructions on your screen.

Setup /a installs the Visio program files and creates the following subdirectory:
Visio\Bin, for Visio product files.

To set up a workstation to run Visio from a network server:

1. On the workstation, from the Start menu, choose Run.
2. Type e:\Visio\setup, where e is the drive letter and \Visio is the directory on the server where the Visio setup program resides.
3. Follow the instructions on the screen.

The workstation setup does the following:

- Installs or updates any Windows system and shared files required by Visio.
- Adds Visio 2000 to the Start Menu.

6. SETTING UP VISIO 2000 ON A NETWORK SERVER FOR LOCAL INSTALLATION TO WORKSTATIONS

You can place Visio 2000 files on a network server by following the steps in the preceding section, "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE." Then, users can connect to the directory and run the Setup program to install Visio on their workstations.

To install Visio 2000 from a network server to a workstation
1. On the workstation, from the Start menu, choose Run.

2. Type f:\visio\setup where f is the drive letter and Visio is the directory on the server where the Visio setup program resides.

3. Follow the instructions on the screen.

4. When Setup prompts you for an installation location, type c:\program files\Visio, where c is the letter assigned to the workstation hard drive and \program files\Visio is the directory on your workstation where the Visio program will reside.

7. DEFINING DEFAULT FILE PATHS FOR VISIO FILES

Users can define default file paths for Visio drawings, templates, add-ons, and filters. To specify these custom paths, choose Options... from the Visio Tools menu, and then click the File Paths tab. File paths defined here are written into the user's registry under the HKEY_LOCAL_MACHINE\Software\Visio\Visio 2000 key. Click the Help button on the File Paths tab for more information.

8. OPENING VISIO FILES ON A NETWORK

Working with and opening Visio files on a network is essentially the same as on an individual workstation. On the network, however, you can make a drawing available to other users and allow them to make changes to the file. You can also protect the file from changes.

* Keep the following issues in mind when using Visio on a network:
You can share stencil files so that multiple users can access them at once. However, when you share stencil files, it is important that users not open them in read/write mode. (When a Visio drawing file is opened in read/write mode, no other network user can access the file.)

By default, the read-only attribute is set for stencil files to prevent users from opening them in read/write mode. You can also set the network Visio directory to read-only to prevent users from opening the files in read/write mode.

9. USING FILTERS WITH VISIO IN SHARED WINDOWS ENVIRONMENTS

If you are using Visio 2000 in a shared Windows environment in which system files are write-protected, Visio 2000 cannot store custom filter settings. You will need to make changes to any filter defaults each time you use that filter - changes will not be retained from one use to the next.
Visio 2000 Standard Edition
END of Network Installation Instructions

APPENDIX I, Tab 3: Example User to Application Mapping Template

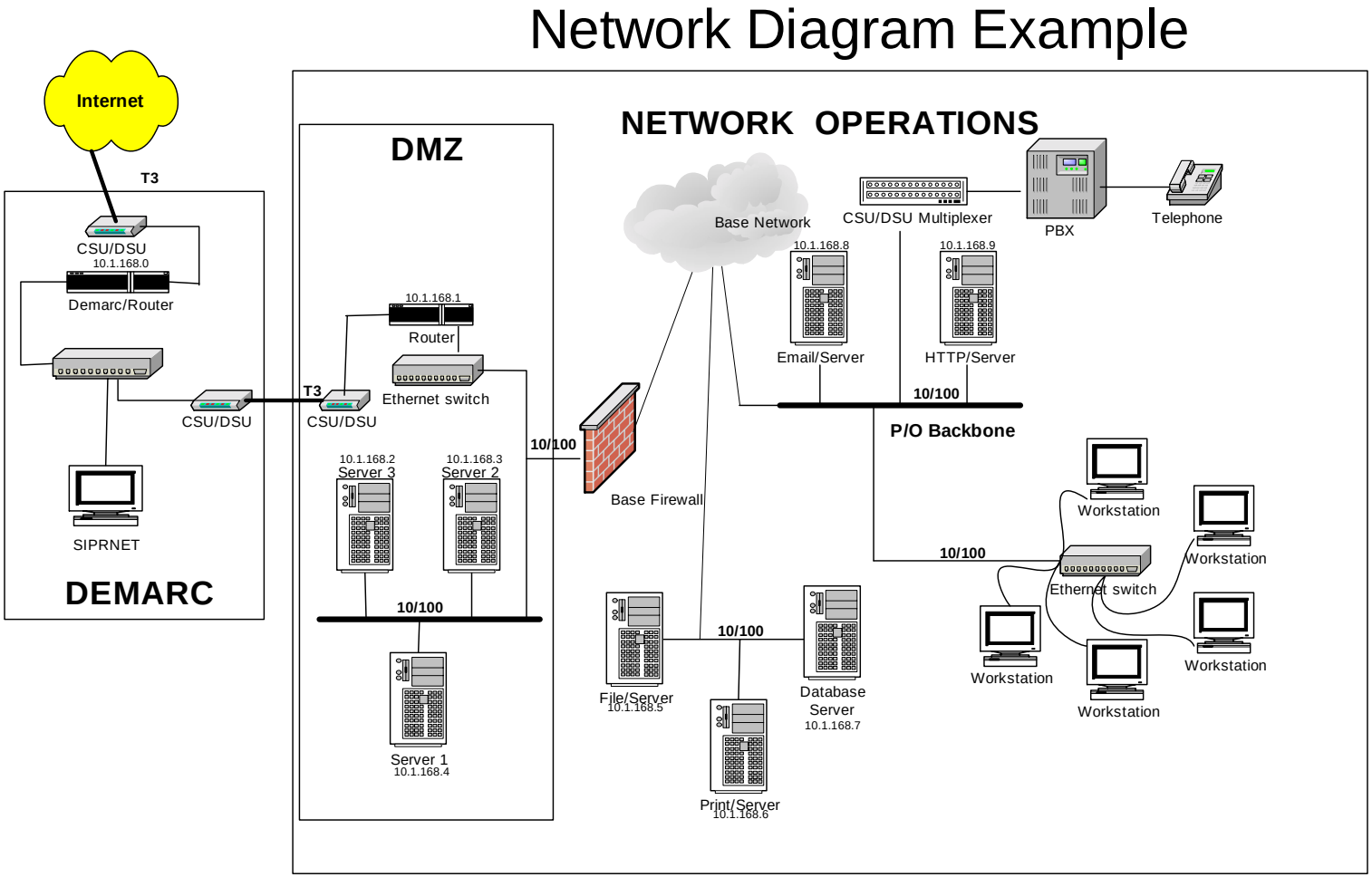
UTAM Master Template

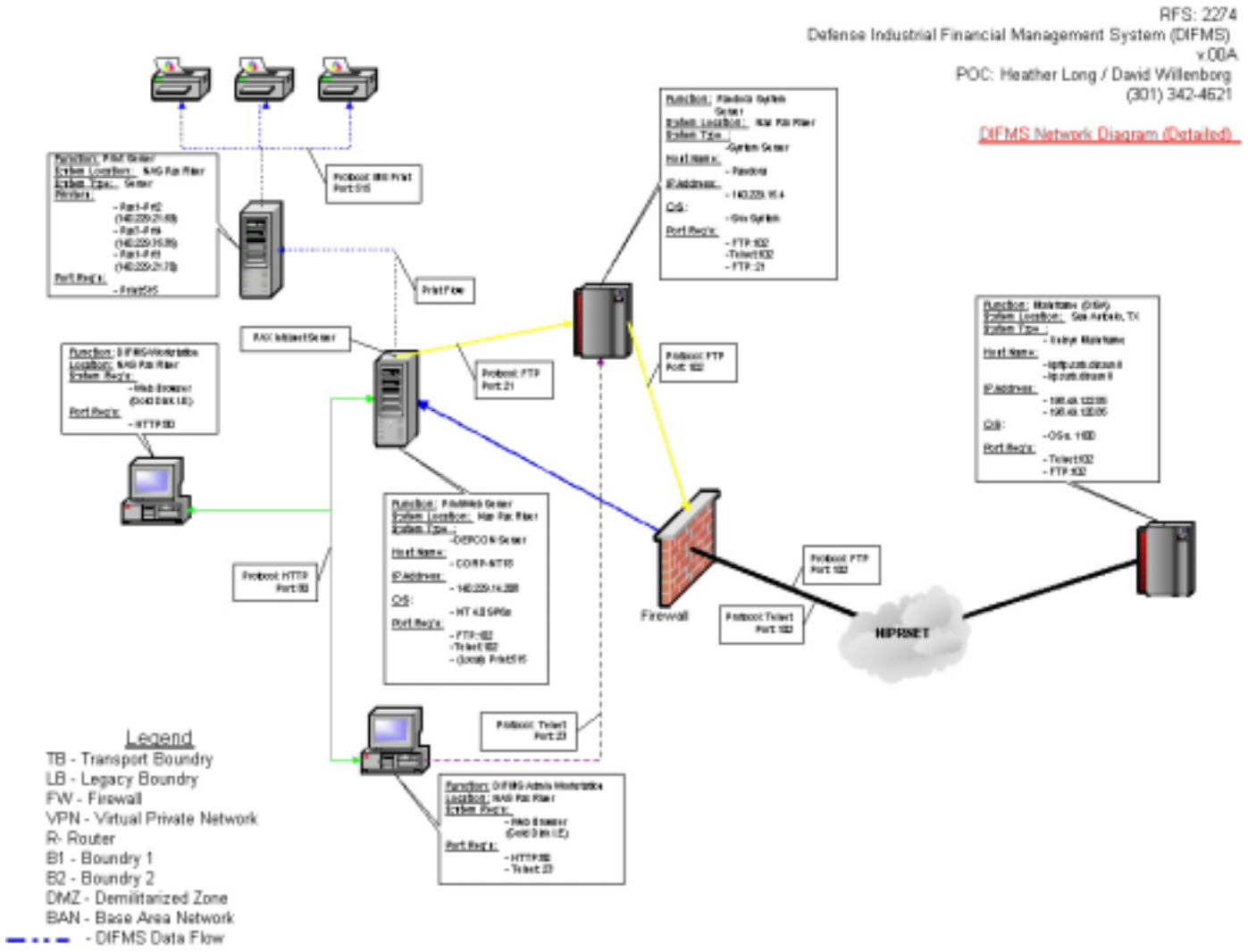
Site:
Date:
POC:
Address:

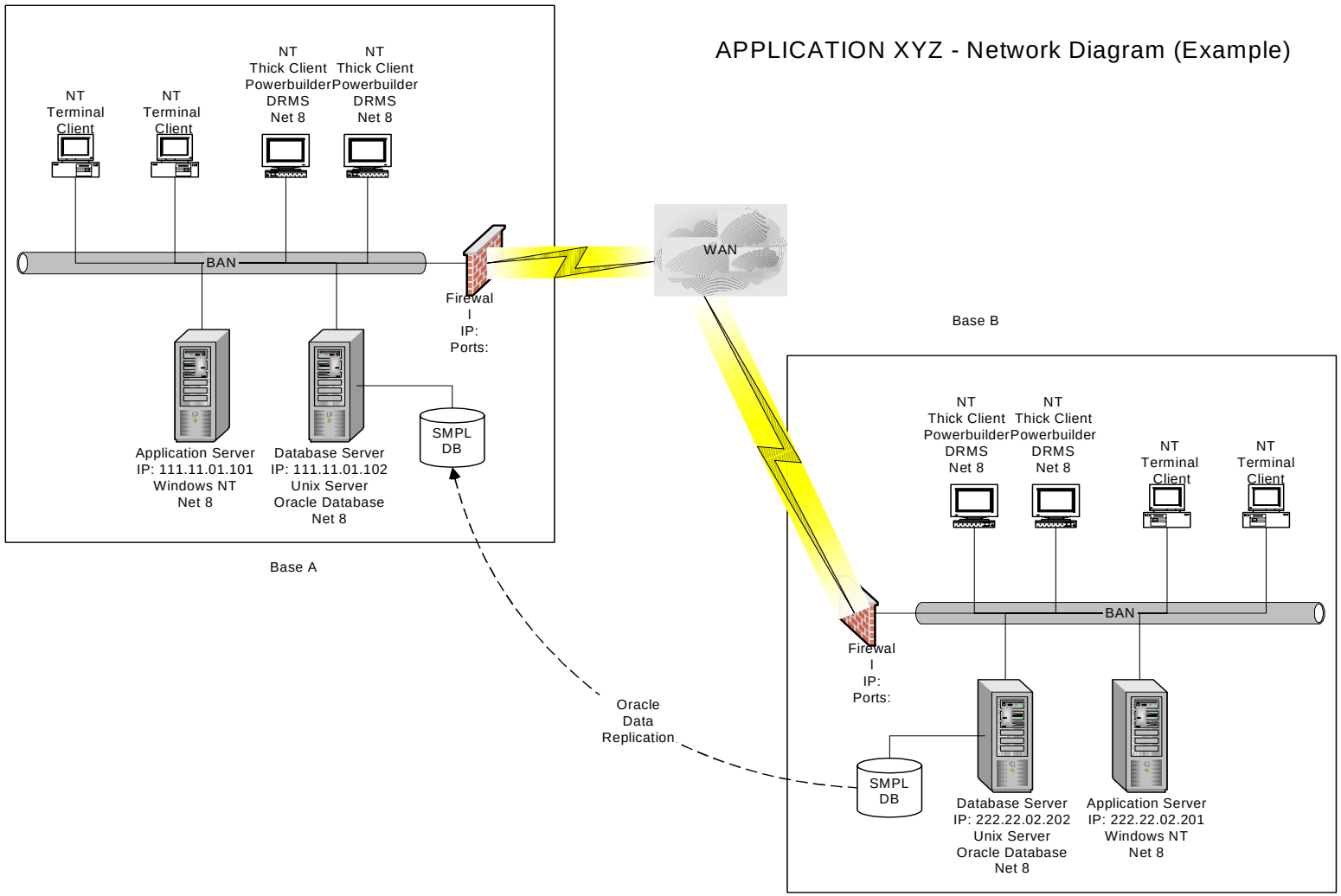
PhoneNumber:
Email:

Application Name	NOVADIGM Application Name	RFS	Last Name	First Name	Middle Initial	User Name	Domain	NetID
Microsoft Word		100	Doe	Joe	E	joe.e.doe.@test.com	cmdhq	doej
			Smith	Jane	A	jane.a.smith@test.com	cmdhq	smithj
			Williams	Will	B	will.b.williams@resource.com	fincmdhq	williamsw
Microsoft Excel		115	Doe	Joe	E	joe.e.doe.@test.com	cmdhq	doej
			Smith	Jane	A	jane.a.smith@test.com	cmdhq	smithj
			Williams	Will	B	will.b.williams@resource.com	fincmdhq	williamsw
Power Point		117	Doe	Joe	E	joe.e.doe.@test.com	cmdhq	doej
			Smith	Jane	A	jane.a.smith@test.com	cmdhq	smithj
			Williams	Will	B	will.b.williams@resource.com	fincmdhq	williamsw
Visio 2000		110	Doe	Joe	E	joe.e.doe.@test.com	cmdhq	doej
			Smith	Jane	A	jane.a.smith@test.com	cmdhq	smithj
			Williams	Will	B	will.b.williams@resource.com	fincmdhq	williamsw

APPENDIX I, Tab 4: Example Network Diagram




RFS: 2274
Defense Industrial Financial Management System (DIFMS)
v.00A
POC: Heather Long / David Willenborg
(301) 342-4621
DIFMS Network Diagram (Detailed)
Firewall
NIPRNET
Legend
TB - Transport Boundry
LB - Legacy Boundry
FW - Firewall
VPN - Virtual Private Network
R- Router
B1 - Boundry 1
B2 - Boundry 2
DMZ - Demilitarized Zone
BAN - Base Area Network
- DIFMS Data Flow


APPLICATION XYZ - Network Diagram (Example)
NT Terminal Client
NT Terminal Client
NT Thick Client Powerbuilder DRMS Net 8
NT Thick Client Powerbuilder DRMS Net 8
BAN
Firewal l IP: Ports:
WAN
Application Server IP: 111.11.01.101 Windows NT Net 8
Database Server IP: 111.11.01.102 Unix Server Oracle Database Net 8
SMPL DB
Base A
Base B
NT Thick Client Powerbuilder DRMS Net 8
NT Thick Client Powerbuilder DRMS Net 8
NT Terminal Client
NT Terminal Client
BAN
Firewal l IP: Ports:
Oracle Data Replication
SMPL DB
Database Server IP: 222.22.02.202 Unix Server Oracle Database Net 8
Application Server IP: 222.22.02.201 Windows NT Net 8

APPENDIX I, Tab 5: Example of DII/COE Installation Procedures

Defense Information Infrastructure (DII)

Common Operating Environment (COE)

Installation Procedures (IP) for
<name and version of software/segment>

<Document Version (if applicable)>

<Date>

Prepared for:

Defense Information Systems Agency

Table of Contents

<< GENERATE THE TABLE OF CONTENTS HERE >>

To generate the Table of Contents:

1. From the Insert menu select *Index* and *Tables*
2. Select the *Table of Contents* tab
3. Highlight *Custom Style* in the formats window, and the preview window will show the headings used
4. Click on "OK" to generate the Table of Contents

List of Tables

<< GENERATE THE LIST OF TABLES HERE >>

To generate the List of Tables:

1. From the Insert menu select *Index* and *Tables*
2. Select the *Table of Figures* tab
3. Highlight *Table* in the Caption Label window
4. Highlight *Custom Style* in the formats window, and the preview window will show the headings used
5. Click on "OK" to generate the List of Tables

List of Figures

<< GENERATE THE LIST OF FIGURES >>

To generate the List of Figures:

1. From the Insert menu select *Index* and *Tables*
2. Select the *Table of Figures* tab
3. Highlight *Figure* in the Caption Label window
4. Highlight *Custom Style* in the formats window, and the preview window will show the headings used
5. Click on "OK" to generate the List of Figures

Notes on Using the Template

1. Refer to Section 3.1 and 3.2 of the *DII COE Developer Documentation Requirements* for format requirements and guidelines for using the templates.
2. This template has been formatted for a small document (12 pages or less). Section headings are left adjusted (refer to Section 3.1.6 of the *DII COE Developer Documentation Requirements*) and are not required to begin on a new odd page.

1. SCOPE

This section shall be divided into the following paragraphs.

1.1 IDENTIFICATION

This paragraph shall contain a full identification of the system and the software. It must provide the name(s), title(s), abbreviation(s), version number(s), and the release number(s). Identification must include the operating system platform(s) to which this document applies.

1.2 System Overview

This paragraph shall provide a brief description of the general nature, purpose, and function of the system/software.

Provide references to additional information sources. Include documentation that may assist the user when problems are encountered. Identify each document-by-document number, title, version/revision, date, and source. Provide a point of contact to be used for reporting problems. Include facilities or organizations equipped to help in the event problems are encountered during installation. Identify organizations with mailing address, telephone number, and fax number, and Web page or Internet address, as available.

2. Referenced Documents

Provide a list of documents referenced in this document. List each document-by-document number, title, version/revision, and date. Identify the source for all documents not available through the Government.

3. System Environment

Describe the system environment necessary to perform the installation of the software in this section. Include system and software configuration information, identify dependencies and compatibility issues, and provide any procedures that must be performed prior to installing the software.

3.1 System Requirements

3.1.1 Hardware Requirements

Identify all system hardware resources required to perform the software installation by name, number, type, size, etc. Provide the RAM and hard disk space required by the software/segment. Provide other requirements for computers, memory, drives, and other devices or components, as applicable.

3.1.2 Operating System Requirements

Identify the operating system and related components required to perform the software installation by names, version numbers, and release numbers, as applicable.

3.1.3 Kernel Requirements

Identify the DII COE Kernel version required to perform the software installation by name, version number, and release number, as applicable.

3.2 System and Site Preparations

Describe the system and site preparations that need to be performed prior to installing the software. Provide procedures for setting up the hardware and software, as needed. Identify hardware/software dependencies and exceptions to configuration, as applicable.

3.2.1 System Configuration

List any software or hardware components that must be installed and configured prior to the installation of the software (e.g., Telecom, Distributed Computing Environment (DCE), etc.). This section may cover requirements for upgrading specific system software with version dependencies.

3.2.2 Operating System Preparation

Provide procedures or information, if any, needed to prepare the operating system. Provide specific system requirements prior to installation (e.g., security, system privileges).

3.2.3 Tape/Disk Preparation

Provide procedures or information needed to prepare the tape or disk drive and related media, as applicable. Identify the physical media containing the software. Describe the disk partitioning and library set-ups that may be required.

4. Installation Instructions

Provide the step-by-step procedure and instructions for installing, configuring, and initializing the system software or segment into the appropriate libraries using the COE approved guideline for segment installation and verification.

4.1 Media Booting Procedure

Provide instruction for booting the media containing the software, as needed, with specific options when required for the installation.

4.2 Installation Procedures

Provide the step-by-step procedures for configuring and installing the software. Provide instructions on how to load or download the software or segment into specific libraries using the DII COE approved guidelines for segment installation and verification.

4.3 Installation of Upgrades

Provide the step-by-step procedures and instructions for upgrading already installed software with new versions or patches. Identify the loading or downloading sequence and options for the software or segment installation.

4.4 Installation Verification

Describe procedures or a method (such as a checklist) for determining if the software installation was successful. This section may also describe and provide instructions for any software verification routines or programs provided, if any.

4.5 Initializing the Software

Describe the steps to be performed at the completion of the software installation. Include the procedures required for the initialization of system and software program operations.

4.6 List of Changes and Enhancements

Provide a brief description of the changes, enhancements, and fixes (patches) incorporated into this version of the software. Reference the applicable SVD for a detailed list of the software changes.

4.7 Important Considerations

Provide any security, licensing, privacy, and/or safety precautions and instruction relevant to the software being installed. This section may also provide critical back up and archiving instruction.

5. Notes

Provide general information to assist in the understanding of this document. This section may include a list of acronyms and abbreviations, and a list of terms and definitions.

6. Documentation Improvement and Feedback

Comments and other feedback on this document should be directed to the DII COE Hotline:

Phone: 703-735-8681
Fax.: 703-735-3080

Email: HotlineC@ncr.disa.mil

A. Appendices

Appendices may be used to provide additional information published separately for convenience in document maintenance. The appendices shall be referenced in the main body of the document, where applicable.

APPENDIX J: Ready to Deploy (RTD)

Navy Central Design Activities that have completed development of the release and are prepared to deploy that release in NMCI will use this form.

SECTION 1 - INFORMATION ON CENTRAL DESIGN ACTIVITY INITIATING REQUEST	
1. Full Name:	
2. E-Mail Address:	
3. Commercial Telephone Number:	4. DSN Telephone Number:
Remarks:	

SECTION 2 - ACTIVITY/COMMAND INFO & POINT OF CONTACT (POC)		
5. Activity/Command Name:		
6. City:	7. State:	8. Zip Code:
9. Activity/Command UIC:		
10. POC Full Name:		
11. POC E-Mail Address:		
12. POC Commercial Phone Number:	13. DSN Phone Number:	
Remarks:		

SECTION 3 - EXISTING (PARENT) APPLICATION INFORMATION		
14. Application Full Name:	15. Acronym:	16. Version:
17. RFS Number:	18. Is this a CDA RFS: Yes ☐ No ☐	
19. Does the application have a waiver? Yes ☐ No ☐ If Yes, attach a copy of the waiver approval to the RTD.	20. Type of application: ☐ COTS ☐ GOTS	
21. Is this a FAM designated enterprise application? Yes ☐ No ☐		
22 Is the existing application being replaced? Yes ☐ No ☐		
Comments:		

SECTION 4 - RELEASE INFORMATION		
23. Release Full Name:	24. Acronym:	25. Version:
26. Does the CDA have written approval from the FAM to develop? Yes ☐ No ☐. If No, the CDA must obtain written approval. If Yes, attach copy of the approval.		
27. Is this release replacing the parent application? Yes ☐ No ☐.		
28. What type of release plan is requested to deploy the release? (See Chapter 2 of NRD2G) ☐ Planned Annual Release ☐ Planned Point Release ☐ Unplanned Emergency/Urgent Release	29. Does the release have Required Deployment Date (RDD)? Yes ☐ No ☐. If Yes, enter the RDD _____(DD/MM/YYYY)	
30. Is this a mandated release? Yes ☐ No ☐. If yes, indicate type and provide comments.		
Remarks:		
31. Are there any special requirements necessary to support this release? Yes ☐ No ☐. If Yes, provide information below to support special requirements.		

SECTION 5 - SPONSORING ECHELON II REVIEW/APPROVAL		
32. Recommendation on CDA RTD: Approved ☐ Disapproved ☐. Provide comment in box below.		
Comment:		
33. Recommendation on CDA prioritization request: Schedule release to meet stated Release Deployment Date (RDD): Yes ☐ No ☐. If no, mark one of the options listed below.		
Planned Annual Release ☐	**Planned Point Release** ☐	**Unplanned Emergency/Urgent** ☐

SECTION 6 – NETWARCOM REVIEW/APPROVAL TO DEPLOY	
34. ☐ Approved ☐ Disapproved	35. Date of action: _____(DD/MMM/YYYY)
Comment: (Mandatory comment if RTD is disapproved).	
36. Action taken on CDA prioritization request: Schedule release to meet stated Release Deployment Date (RDD): Yes ☐ No ☐. If no, mark one of the options listed below.	
Planned Annual Release ☐	**Planned Point Release** ☐	**Unplanned Emergency/Urgent** ☐

SECTION 7 – NMCI RELEASE PRIORITIZATION MANAGER		
37. Has an adequate review of the release/application requirements been completed? Yes ☐ No ☐. If Yes, provide information below to support special requirements.		
Comments:		
38. NRPM Recommendation: Approved ☐ Disapproved ☐		
Planned Annual Release ☐	**Planned Point Release** ☐	**Unplanned Emergency/Urgent** ☐
NPRM Priority Description:		

SECTION 8 - NMCI RELEASE SCHEDULING MANAGER	
39. Are there any special requirements necessary to support this release/application? Yes ☐ No ☐	
Comments:	
40. NRSM Recommendation: Approved ☐ Disapproved ☐	
41. Schedule Submission Date: (DD/MMM/YYYY)	42. Required Deployment Date: (DD/MMM/YYYY)

REQUEST TO DEPLOY (RTD)

AUTHORITY:

PRINCIPLE PURPOSE: To initial action to request authority to develop and deploy an application

ROUTINE USE: This form will by used by both government and contractor, to provide services under the provisions of the NMCI contract. The information provided is necessary, to assist the approving authority in determining the proper action to be taken for the deployment of a release or application.

DISCLOSURE:

INSTRUCTIONS

SECTION 1 – INFORMATION ON CENTRAL DESIGN ACTIVITY INITIATING REQUEST

ITEMS 1 through 4. Self-explanatory.

SECTION 2 - ACTIVITY/ COMMAND INFO & POINT OF CONTACT

ITEMS 5 through 13 Self-explanatory.

SECTION 3 - EXISTING (PARENT) APPLICATION INFORMATION

ITEMS 14 through 22. Self-explanatory.

To avoid confusion, Information entered must be identical to information in the ISF Tools database. Use the Remarks section to enter additional information pertaining to the application. Enter information of applications that have an approved waiver in the remarks block.

SECTION 4-RELEASE INFORMATION

ITEMS 23 through 31. Self-explanatory.

All applications must have a CDA or a designated POC. Be as specific as possible.

SECTION 5 – SPONSORING ECHELON II REVIEW/APPROVAL

ITEMS 32 through 33. Self-explanatory

This information pertains to a new release/application to be developed.

List specific special application requirements in the remarks block.

SECTION 6 - NETWARCOM REVIEW/APPROVAL

ITEMS 34 through 36. Self-explanatory.

List specific special application requirements in the remarks block.

SECTION 7- NMCI RELEASE PRIORITIZATION MANAGER

ITEMS 37 through 38. Self-explanatory

List specific special application requirements in the remarks block.

SECTION 8 - NMCI RELEASE SCHEDULING MANAGER

ITEMS 39 through 42. Self-explanatory

List specific special application requirements in the remarks block.